WatchGuard® System Manager User Guide

Fireware® v8.3
Fireware® Pro v8.3

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the appendix of this User Guide.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Management Software: 8.3
Appliance Software: Fireware® 8.3 and Fireware Pro 8.3
Document Version: 8.3-352-2671-001

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

Contents iii

CHAPTER 1 Introduction 1
- About Fireware and Fireware Pro 1
- Fireware Features and Tools 2
- WatchGuard System Manager (WSM) User Interface 4
  - *About the WatchGuard toolbar* 4
  - *About the WatchGuard System Manager Window* 4
  - *Device status* 5
  - *Connection status* 6

CHAPTER 2 Getting Started 9
- Installing WatchGuard System Manager 9
  - *Installation requirements* 9
  - *Collecting network information* 10
  - *Selecting a firewall configuration mode* 11
  - *Selecting where to install server software* 13
  - *Setting up the management station* 13
  - *Backing up your previous configuration* 14
- Quick Setup Wizard 14
  - *Firebox X Core and Peak e-Series Web Quick Setup Wizard* 15
  - *Quick Setup Wizard* 16
- Putting the Firebox into Operation 16
- Starting WatchGuard System Manager 17
  - *Connecting to a Firebox* 17
  - *Disconnecting from a Firebox* 18
  - *Starting security applications* 18
- After Your Installation 19
  - *Customizing your security policy* 19
  - *Features of the LiveSecurity Service* 19
- Upgrading to a New Version of Fireware 20

Installation Topics 20
Installing WatchGuard Servers on computers with desktop firewalls 20
Adding secondary networks to your configuration 21
Dynamic IP support on the external interface 21
Entering IP addresses 22
Installing the Firebox cables 22
CHAPTER 3 Service and Support 23
LiveSecurity Service Solutions 23
LiveSecurity Service Broadcasts 24
Activating LiveSecurity Service 25
LiveSecurity Service Self Help Tools 25
WatchGuard Users Forum 26
Online Help 27
Starting WatchGuard online Help 27
Searching for information 27
Copy the online Help system to more computers 27
Product Documentation 28
Technical Support 28
LiveSecurity Service technical support 28
LiveSecurity Gold 29
Firebox Installation Service 29
VPN Installation Service 29
Training and Certification 29
CHAPTER 4 Monitoring Firebox Status 31
Starting Firebox System Manager 31
Connecting to a Firebox 31
Opening Firebox System Manager 32
Firebox System Manager Menus and Toolbar 32
Setting refresh interval and pausing the display 34
Seeing Basic Firebox and Network Status 34
Using the Security Traffic display 35
Monitoring status information 35
Setting the center interface 36
Monitoring traffic, load, and status 36
Firebox and VPN tunnel status 36
Monitoring Firebox Traffic 38
Setting the maximum number of log messages 38
Using color for your log messages 39
Copying log messages 39
Learning more about a traffic log message 40
Clearing the ARP Cache 40
Using the Performance Console 40
Types of counters 40
Defining counters 41

Viewing the performance graph 43
Working with more than one Performance Console graph 44
Viewing Bandwidth Usage 45
Viewing Number of Connections by Policy 46
Viewing Information About Firebox Status 48
Status Report 48
Authentication List 49
Blocked Sites 50
Security Services 51
Using HostWatch 53
The HostWatch window 53
Controlling the HostWatch window 54
Changing HostWatch view properties 55
Adding a blocked site from HostWatch 55
Pausing the HostWatch display 56
CHAPTER 5 Basic Firebox Administration 57
Working with Licenses 57
Activating a new feature 57
Adding licenses 59
Deleting a license 59
Seeing the active features 60
Seeing the properties of a license 61
Downloading a license key 61
Setting NTP Servers 61
Setting a Friendly Name and Time Zone 62
Working with SNMP 62
Enabling SNMP polling 63
Enabling SNMP traps 63
Using MIBs 64
Changing the Firebox Passphrases 64
Recovering a Firebox 65
Resetting a Firebox X e-Series device 65
Resetting a Firebox X Core or Peak (non e-Series) 65
Resetting a Firebox using fbxinstall 66
CHAPTER 6 Basic Configuration Setup 69
Opening a Configuration File 69
Opening a working configuration file 69
Opening a local configuration file 71
Making a new configuration file 71
Saving a Configuration File 71
Saving a configuration to the Firebox 72
Saving a configuration to a local hard drive 72
About Firebox Backup Images 72
Creating a Firebox backup image 72

Restoring a Firebox backup image 73
Working with Aliases 73
Creating an alias 74
Using Global Settings 75
VPN 75
ICMP error handling 76
TCP SYN checking 76
TCP maximum segment size adjustment 77
Authentication settings 77
Creating Schedules 77
Managing a Firebox from a Remote Location 78
CHAPTER 7 Logging and Notification 81
Setting Up the Log Server 82
Changing the Log Server encryption key 82
Setting up the Firebox for a Designated Log Server 83
Adding a Log Server for a Firebox 83
Setting Log Server priority 84
Activating syslog logging 84
Enabling advanced diagnostics 85
Setting Global Logging and Notification Preferences 86
Log file size and rollover frequency 87
Setting when log files rollover 87
Scheduling automated reports 88
Controlling notification 89
Starting and stopping the Log Server 89
About Log Messages 89
Types of Log Messages 90
Log File Names and Locations 90
Starting LogViewer 91
LogViewer Settings 92
Using LogViewer 93
Creating a Search Rule 93
Searching in LogViewer 94
Viewing the current log file in LogViewer 94
Copying LogViewer data 94
Consolidating log files 95
Updating .wgl log files to .xml format 95
CHAPTER 8 Network Setup and Configuration 97
Changing Firebox Interface IP Addresses 98
Configuring the external interface 100
About Multiple WAN Support 102
About multi-WAN in round robin order 102
About WAN Failover 103
About multi-WAN with the routing table 103

Configuring multiple WAN support 104
Adding Secondary Networks 105
Adding WINS and DNS Server Addresses 107
Configuring Dynamic DNS 108
Configuring Routes 110
Adding a network route 110
Adding a host route 110
Setting Firebox Interface Speed and Duplex 111
Configuring Related Hosts 111
CHAPTER 9 Working with Firewall NAT 113
Using Dynamic NAT 114
Adding firewall dynamic NAT entries 114
Reordering dynamic NAT entries 115
Policy-based dynamic NAT entries 115
Using 1-to-1 NAT 116
Defining a 1-to-1 NAT rule 117
Configuring firewall 1-to-1 NAT 118
Configuring policy-based 1-to-1 NAT 118
Configuring policy-based dynamic NAT 119
Configuring Static NAT for a Policy 119
CHAPTER 10 Implementing Authentication 121
How User Authentication Works 121
Using authentication from the external network 122
Using authentication through a gateway Firebox to another Firebox 122
Authentication server types 123
Using a backup authentication server 123
Configuring the Firebox as an Authentication Server 123
About Firebox authentication 123
Setting up the Firebox as an authentication server 125
Using a local user account for Firewall user, PPTP, and MUVPN authentication 126
Configuring RADIUS Server Authentication 127
Configuring SecurID Authentication 128
Configuring LDAP Authentication 129
Configuring Active Directory Authentication 131
Configuring a Policy with User Authentication 132
CHAPTER 11 Firewall Intrusion Detection and Prevention 135
Using Default Packet Handling Options 135
Spoofing attacks 136
IP source route attacks 136
"Ping of death" attacks 136
Port space and address space attacks 137
Flood attacks 137
Unhandled packets 137
Distributed denial of service attacks 137

Setting Blocked Sites 138
Blocking a site permanently 138
Blocking spyware sites 139
Using an external list of blocked sites 140
Creating exceptions to the Blocked Sites list 140
Setting logging and notification parameters 140
Blocking sites temporarily with policy settings 141
Blocking Ports 142
Blocking a port permanently 143
Automatically blocking IP addresses that try to use blocked ports 143
Setting logging and notification for blocked ports 143
CHAPTER 12 Configuring Policies 145
Creating Policies for your Network 145
Adding Policies 146
Changing the Policy Manager View 146
Adding a policy 147
Making a custom policy template 148
Adding more than one policy of the same type 150
Deleting a policy 150
Configuring Policy Properties 150
Setting access rules, sources, and destinations 151
Setting a proxy action 152
Setting logging properties 153
Configuring static NAT 154
Setting advanced properties 156
Setting Policy Precedence 157
Using automatic order 157
Setting precedence manually 159
CHAPTER 13 Configuring Proxied Policies 161
Defining Rules 161
Adding rulesets 162
Using the advanced rules view 163
Customizing Logging and Notification for Proxy Rules 164
Configuring log messages and notification for a proxy policy 164
Configuring log messages and alarms for a proxy rule 164
Using dialog boxes for alarms, log messages, and notification 164
Configuring the SMTP Proxy 166
Configuring general settings 167
Configuring ESMTP parameters 168
Configuring authentication rules 169
Defining content type rules 170
Defining file name rules 170
Configuring the Mail From and Mail To rules 170
Defining header rules 170
Defining antivirus responses 170

Changing the deny message 171
Configuring the IPS (Intrusion Prevention System) for SMTP 171
Configuring spamBlocker 171
Configuring proxy and antivirus alarms for SMTP 171
Configuring the FTP Proxy 172
Configuring general settings 172
Defining commands rules for FTP 173
Setting download rules for FTP 173
Setting upload rules for FTP 173
Enabling intrusion prevention for FTP 173
Configuring proxy alarms for FTP 174
Configuring the HTTP Proxy 174
Configuring settings for HTTP requests 174
Configuring general settings for HTTP responses 177
Setting header fields for HTTP responses 177
Setting content types for HTTP responses 177
Setting cookies for HTTP responses 177
Setting HTTP body content types 178
Defining antivirus responses for HTTP 178
Changing the deny message 178
Enabling intrusion prevention for HTTP 179
Defining proxy and antivirus alarms for HTTP 179
Configuring the DNS Proxy 180
Configuring general settings for the DNS proxy 180
Configuring DNS OPcodes 181
Configuring DNS query types 181
Configuring DNS query names 182
Enabling intrusion prevention for DNS 182
Configuring DNS proxy alarms 182
Configuring the TCP Proxy 183
Configuring general settings for the TCP proxy 183
Enabling intrusion prevention for TCP 183
CHAPTER 14 Generating Reports of Network Activity 185
Creating and Editing Reports 185
Starting Historical Reports 185
Starting a new report 186
Editing an existing report 187
Deleting a report 187
Viewing the reports list 187
Backing up report definition files 187
Setting Report Properties 187
Specifying a report time interval 187
Specifying report sections 188
Consolidating report sections 189
Setting report properties 190
Viewing network interface relationships 190

Exporting Reports 190
Exporting reports to HTML format 191
Exporting reports to NetIQ format 191
Using Report Filters 191
Creating a new report filter 192
Editing a report filter 192
Deleting a report filter 193
Applying a report filter 193
Running Reports 193
Report Sections and Consolidated Sections 193
Report sections 193
Consolidated sections 196
CHAPTER 15 Management Server Setup and Administration 197
WatchGuard Management Server Passphrases 197
Setting Up the Management Server 199
Changing the Management Server Configuration 200
Adding or removing a Management Server license 200
Recording diagnostic log messages for the Management Server 201
Configuring the Certificate Authority 201
Configuring properties for the CA certificate 201
Configuring properties for client certificates 202
Configuring properties for the Certificate Revocation List (CRL) 203
Recording diagnostic log messages for the Certificate Authority service 204
Backing up or Restoring the Management Server Configuration 204
Moving the WatchGuard Management Server to a New Computer 205
CHAPTER 16 Using the Management Server 207
Connecting to a Management Server 207
Managing Devices with the Management Server 208
Configuring a Firebox X Core or X Peak Running Fireware as a Managed Client 208
Configuring a Firebox III or Firebox X Core Running WFS as a Managed Client 210
Configuring a Firebox X Edge as a Managed Client 211
Configuring a Firebox SOHO 6 as a Managed Client 212
Adding Devices to the Management Server 213
Using the Device Management Page 216
Viewing the Firebox management page 216
Configuring Firebox management properties 218
Updating the device 218
Adding a VPN resource 219
Starting Firebox tools 219
Adding a Firebox VPN tunnel 220
Monitoring VPNs 220
CHAPTER 17 Managing Certificates and the Certificate Authority 221
Public Key Cryptography and Digital Certificates 221
PKI in a WatchGuard VPN 222

MUVPN and certificates 222
Managing the Certificate Authority 222
Managing certificates with the CA Manager 223
CHAPTER 18 Introduction to VPNs 225
Tunneling Protocols 226
IPSec 226
PPTP 226
Encryption 226
Selecting an encryption and data integrity method 227
Authentication 227
Extended authentication 227
Selecting an authentication method 227
IP Addressing 228
Internet Key Exchange (IKE) 228
Network Address Translation and VPNs 229
Access Control 229
Network Topology 229
Meshed networks 229
Hub-and-spoke networks 230
Tunneling Methods 231
WatchGuard VPN Solutions 232
Remote User VPN with PPTP 232
Mobile User VPN 232
Branch Office Virtual Private Network (BOVPN) 233
VPN Scenarios 234
Large company with branch offices: WatchGuard System Manager 234
Small company with telecommuters: MUVPN 235
Company with remote employees: MUVPN with extended authentication 235
CHAPTER 19 Configuring Managed VPN Tunnels 237
Configuring a Firebox as a Managed Firebox Client 237
Adding Policy Templates 237
Get the current templates from a device 238
Make a new policy template 238
Adding resources to a policy template 239
Adding Security Templates 239
Making Tunnels Between Devices 240
Using the drag-and-drop procedure 240
Using the Add VPN wizard without drag-and-drop 240
Editing a Tunnel 241
Removing Tunnels and Devices 241
Removing a tunnel 241
Removing a device 241
CHAPTER 20 Configuring BOVPN with Manual IPSec 243
Before You Start 243

Configuring a Gateway 243
Adding a gateway 243
Editing and deleting gateways 246
Making a Manual Tunnel 246
Editing and deleting a tunnel 249
Making a Tunnel Policy 250
Setting up Outgoing Dynamic NAT through a BOVPN Tunnel 250
CHAPTER 21 Managing the Firebox X Edge and Firebox SOHO 253
Working with Devices on a Management Server 254
Preparing a new or factory default Firebox X Edge for management 254
Preparing an installed Firebox X Edge for management 255
Preparing a Firebox SOHO 6 for management 256
Adding Firebox X Edge and SOHO 6 devices to a Management Server 257
Scheduling Firebox X Edge Firmware Updates 259
Viewing and deleting firmware updates 261
Using the Firebox X Edge Management Page 261
Viewing the Firebox X Edge management page 261
Configuring Firebox X Edge management properties 262
Updating the device 263
Adding a VPN Resource 263
Starting Firebox X Edge tools 264
Adding a Firebox X Edge VPN Tunnel 264
Using the Firebox X Edge Policy section 265
Using the Firebox SOHO 6 Management Page 265
Viewing the SOHO 6 management page 265
Configure Firebox SOHO 6 management properties 266
Updating the device 266
Adding a VPN Resource 267
Starting Firebox SOHO 6 tools 267
Adding a Firebox SOHO 6 VPN Tunnel 268
Creating and Applying Edge Configuration Templates 268
Adding a pre-defined policy with the Add Policy wizard 269
Adding a custom policy with the Add Policy wizard 270
Cloning an Edge Configuration Template 271
Applying an Edge Configuration Template to devices 271
Managing Firebox X Edge Network Settings 273
Using Aliases 275
Naming aliases on the Management Server 276
Defining aliases on a Firebox X Edge 277
CHAPTER 22 Configuring RUVPN with PPTP 279
Configuration Checklist 279
Encryption levels 279
Configuring WINS and DNS Servers 280
Enabling RUVPN with PPTP 281

Enabling extended authentication 281
Adding IP Addresses for RUVPN Sessions 281
Adding New Users to the PPTP_Users Authentication Group 282
Configuring Policies to Allow Incoming RUVPN Traffic 283
By individual policy 283
Using the Any policies 284
Preparing the Client Computers 284
Installing MSDUN and service packs 285
Creating and Connecting a PPTP RUVPN on Windows XP 285
Creating and Connecting a PPTP RUVPN on Windows 2000 286
Running RUVPN and accessing the Internet 286
Making outbound PPTP connections from behind a Firebox 287
CHAPTER 23 Controlling Web Site Access with WebBlocker 289
Installing the Software Licenses 289
Getting Started with WebBlocker 290
Automating WebBlocker database downloads 291
Activating WebBlocker 291
Configuring WebBlocker 293
Adding new servers 294
Selecting categories to block 294
Defining WebBlocker exceptions 295
Defining advanced WebBlocker options 296
Scheduling a WebBlocker Action 297
CHAPTER 24 Configuring spamBlocker 299
About spamBlocker 299
spamBlocker actions 299
spamBlocker tags 300
spamBlocker categories 300
Installing the Software License 300
Activating spamBlocker 301
Configuring spamBlocker 303
Adding spamBlocker exceptions 304
Creating Rules for Bulk and Suspect E-mail on E-mail Clients 304
Sending spam or bulk e-mail to special folders in Outlook 304
Reporting False Positives and False Negatives 305
Monitoring spamBlocker Activity 305
Customizing spamBlocker Using Multiple Proxies 306
CHAPTER 25 Using Signature-Based Security Services 307
Installing the Software Licenses 308
About Gateway AntiVirus 308
Activating Gateway AntiVirus 309
Configuring Gateway AntiVirus 310
Creating alarms or log entries for antivirus responses 311

Configuring GAV engine settings 311
Configuring the GAV signature server 312
Using Gateway AntiVirus with more than one proxy 312
Unlocking an attachment locked by Gateway AntiVirus 312
Getting Gateway AntiVirus Status and Updates 313
Seeing service status 313
Updating GAV signatures or the GAV engine manually 314
Updating the antivirus software 314
Activating Intrusion Prevention (IPS) 314
Configuring Intrusion Prevention 316
Configuring intrusion prevention for HTTP or TCP 317
Configuring Intrusion Prevention for FTP, SMTP, or DNS 319
Configuring the signature server 320
Configuring signature exceptions 320
Copying IPS settings to other policies 320
Getting Intrusion Prevention Service Status and Updates 321
Seeing service status 321
Updating signatures manually 322
CHAPTER 26 Advanced Networking 323
Creating QoS Actions 323
Applying QoS actions to policies 325
Using QoS in a multiple WAN environment 325
Dynamic Routing 326
Using RIP 326
RIP Version 1 326
RIP Version 2 330
Using OSPF 332
OSPF daemon configuration 332
Configuring Fireware Pro to use OSPF 335
Using BGP 337
CHAPTER 27 High Availability 343
High Availability Requirements 343
Selecting a Primary High Availability Firebox 344
Configuring HA for Firebox X e-Series Devices 344
Configuring the secondary High Availability Firebox 345
Enabling High Availability 345
Configuring HA for Firebox X (non e-Series) Devices 346
Manually Controlling High Availability 347
Backing up an HA configuration 348
Upgrading Software in an HA Configuration 348
Using HA with Signature-based Security Services 348
Using HA with Proxy Sessions 348

APPENDIX A Copyright and Licensing 349
Licenses 355
SSL Licenses 355
Apache Software License, Version 2.0, January 2004 357
PCRE License 359
GNU Lesser General Public License 360
GNU General Public License 365
Sleepycat License 368
Sourcefire License 369
Expat-MIT HTML Parser Toolkit License 373
Curl Software MIT-X License 373
APPENDIX B WatchGuard File Locations 375
Default File Locations 376
APPENDIX C Types of Policies 379
Packet Filter Policies 379
Any 379
AOL 380
archie 380
auth 380
BGP 380
Citrix 380
Clarent-gateway 381
Clarent-command 381
CU-SeeMe 382
DHCP-Server or DHCP-Client 382
DNS 382
Entrust 382
finger 383
FTP 383
Gopher 383
GRE 383
HTTP 384
HTTPS 384
HBCI 384
IDENT 384
IGMP 385
IKE 385
IMAP 385
IPSec 385
IRC 386
Intel Video Phone 386
Kerberos v 4 and Kerberos v 5 386
L2TP 386
LDAP 386
LDAP-SSL 387
Lotus Notes 387

MSSQL-Monitor 387
MSSQL-Server 387
MS Win Media 387
NetMeeting 388
NFS 388
NNTP 388
NTP 388
OSPF 389
pcAnywhere 389
ping 389
POP2 and POP3 389
PPTP 390
RADIUS and RADIUS-RFC 390
RADIUS-Accounting and RADIUS-ACCT-RFC 390
RDP 390
RIP 391
RSH 391
RealPlayer G2 391
Rlogin 391
SecurID 392
SMB (Windows Networking) 392
SMTP 392
SNMP 392
SNMP-Trap 393
*SQL*Net* 393
SQL-Server 393
ssh 393
Sun RPC 393
syslog 394
TACACS 394
TACACS+ 394
TCP 394
TCP-UDP 395
UDP 395
telnet 395
Timbuktu 395
Time 395
traceroute 396
UUCP 396
WAIS 396
WinFrame 396
WG-Auth 397
WG-Firebox-Mgmt 397
WG-Logging 397
WG-Mgmt-Server 397
WG-SmallOffice-Mgmt 398
WG-WebBlocker 398

WHOIS 398
X11 398
Yahoo Messenger 398
Proxied Policies 399
DNS 399
FTP 399
HTTP 399
SMTP 399
TCP Proxy 400

Index 401

CHAPTER 1

Introduction

WatchGuard® System Manager gives you an easy and efficient way to manage your network security. With one computer as a management station, you can show, manage, and monitor each Firebox® device in your network.

WSM supports mixed environments. You can manage different models of Firebox devices that use different versions of appliance software. You can also do centralized management of Firebox X Edge devices.

WSM has three servers that do Firebox management functions:

Management Server

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create VPN (virtual private network) tunnels using a simple drag-and-drop function. The basic functions of the Management Server are:

- Centralized management of VPN tunnel configurations
- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- Protocol translation in support of the WatchGuard SOHO and Firebox X Edge products

Log Server

The Log Server collects log messages from each WatchGuard Firebox. The log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The information collected from firewall devices includes traffic log messages, event log messages, alarms, and diagnostic messages.

WebBlocker Server

The WebBlocker Server operates with the Firebox HTTP proxy to deny user access to specified categories of web sites. The administrator sets the categories of web sites to allow or block during Firebox configuration.

About Fireware and Fireware Pro

WatchGuard® Fireware® is the next generation of security appliance software available from WatchGuard. Appliance software is a software application kept in the memory of your firewall hardware. The Firebox® uses the appliance software with a configuration file to operate.

Your organization's security policy is a set of rules that define how you protect your computer network and the information that passes through it. Fireware appliance software has advanced features to manage security policies for the most complex networks.

Two versions of Fireware are available to WatchGuard® customers:

- Fireware® — This is the default appliance software on Firebox X Core e-Series devices.
- Fireware® Pro — This is the default appliance software on Firebox X Peak e-Series devices. If you have a Firebox X Core, you can purchase a Fireware Pro upgrade. This appliance software has these advanced features for more complex networks:
  - High Availability
  - Advanced networking options that include QoS (quality of service) and dynamic routing

WatchGuard System Manager also includes the software tools you must have to configure and manage a Firebox X device that uses WFS appliance software. WFS appliance software is the default appliance software that shipped with earlier models of the Firebox X Core and Peak. For more information about WFS appliance software, see the *WFS Configuration Guide*.

After a Firebox is put in WSM management, the software automatically identifies which appliance software the Firebox uses. If you select the Firebox and then click an icon on the toolbar, it starts the correct management tool. These tools include:

- Firebox System Manager
- Policy Manager
- HostWatch

For example, if you add a Firebox X700 operating with WFS appliance software to the **Devices** tab of WFS and then click the Policy Manager icon on the WSM toolbar, Policy Manager for WFS automatically starts. If you add a Firebox X700 operating with Fireware appliance software and click the Policy Manager icon, Policy Manager for Fireware starts.

Fireware Features and Tools

WatchGuard® Fireware® and Fireware Pro include many features to improve your network security.

Policy Manager for Fireware

Policy Manager gives you one user interface for basic firewall configuration tasks. Policy Manager includes a full set of preconfigured packet filters and proxies. For example, to apply a packet filter for all Telnet traffic, you add a Telnet packet filter. You can also make a custom packet filter for which you set the ports, protocols, and other parameters. Careful configuration of IPS options can stop attacks such as SYN Flood attacks, spoofing attacks, and port or address space probes.

Firebox System Manager

Firebox® System Manager gives you one interface to monitor all components of your Firebox. From Firebox System Manager, you can monitor the current condition of the Firebox or connect directly to get an update on its configuration.

Network Address Translation

Network address translation (NAT) is a term used for one or more methods of IP address and port address translation. Network administrators frequently use NAT to increase the number of computers

that can operate with only one public IP address. NAT also hides the private IP addresses of computers on your network.

Multi-WAN

Fireware lets you configure a maximum of four Firebox interfaces as external, or WAN, interfaces. You can control the flow of traffic through more than one WAN interface to share the volume of outgoing traffic.

Firebox and third-party authentication servers

WatchGuard® System Manager with Fireware supports five different authentication protocols: Firebox, RADIUS, SecurID, LDAP, and Active Directory.

Signature-based intrusion detection and prevention

A unique set of qualities for a given virus or attack is known as the signature. When a new intrusion attack is identified, the qualities that make the virus or attack unique are identified and recorded and a new signature can be created and distributed. WatchGuard Gateway AntiVirus and Intrusion Prevention Service use these signatures to find viruses and detect intrusion attacks. Service subscribers can schedule automatic or manual updating of their signature sets. The Intrusion Prevention Service operates with all WatchGuard proxies. Gateway AntiVirus operates with the SMTP and HTTP proxies.

VPN creation and management

Fireware technology makes it easier to configure, manage, and monitor many IPSec VPN tunnels to branch offices and end users.

Advanced networking features

The QoS feature in Fireware Pro lets you set priority and bandwidth restrictions for each policy. The Firebox can also use the dynamic route protocols RIP, OSPF, and BGP. These protocols can decrease network maintenance and supply route redundancy.

Note

QoS and the OSPF and BGP protocols are supported in Fireware® Pro only.
The RIP protocol is supported in both Fireware and Fireware Pro.

Web traffic control

The WebBlocker feature uses the HTTP Proxy to apply a filter to Web traffic. You can set the hours in the day that users can get access to different types of web content. You can also set categories of web sites that users cannot browse to.

High Availability

High Availability supplies stateful failover for firewall connections. With High Availability, you can have one Firebox in operation in standby mode, while the other Firebox continues to operate. The standby Firebox automatically takes over firewall operations if the primary Firebox is not able to connect with the Internet.

Note

High Availability is supported in Fireware® Pro only.

WatchGuard System Manager (WSM) User Interface

The basic components of the WatchGuard® System Manager user interface are the WatchGuard toolbar and the WatchGuard System Manager window. This section gives basic information about the user interfaces. See subsequent chapters for more information.

About the WatchGuard toolbar

You use the WatchGuard toolbar to start, stop, and configure these servers:

- Management Server
- Log Server
- WebBlocker Server

The WatchGuard toolbar is one of the toolbars at the bottom of your computer screen. If you have not installed any WatchGuard server software on your management station, you do not see the WatchGuard toolbar.

From left to right, the icons on the toolbar manage these servers:

- Log Server — This server collects log messages, event messages, alarms, and diagnostic messages from Firebox® X Edge, FSM, and Fireware®-based devices in XML (plain text) format. For information on Log Server, see the "Logging and Notification" chapter in this guide.
- Management Server — The Management Server operates on a Windows computer. To migrate a DVCP server from a Firebox to your computer, see the *Migration Guide*.
- WebBlocker Server — This server operates with the Firebox HTTP proxy to limit user access to applicable web sites. For information on WebBlocker, see the "Controlling Web Site Access with WebBlocker" chapter.

About the WatchGuard System Manager Window

The WatchGuard® System Manager window has two tabs that you can use to monitor and manage your network:

The WatchGuard® System Manager window has two tabs at the top of the screen:

Device Status

This tab shows the status of devices connected to WatchGuard System Manager. The information that appears includes the status, IP address, and MAC address for each Ethernet interface, and the installed certificates. It also includes the status of all VPN tunnels that are configured in System Manager.

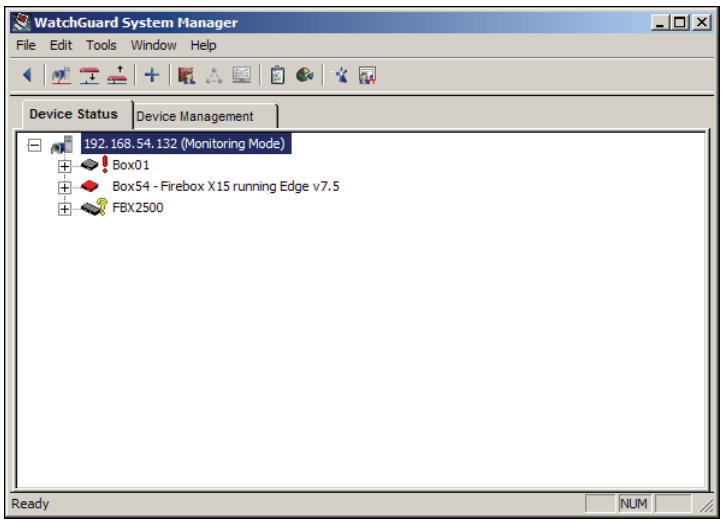
The devices that appear on this tab are connected directly to WatchGuard System Manager.

Device Management

This tab shows a navigation pane and an information pane. The navigation pane shows the connected WatchGuard Management Servers and their devices, managed VPNs, and managed Firebox® X Edge configurations. The information pane shows more information for any item you select in the navigation pane.

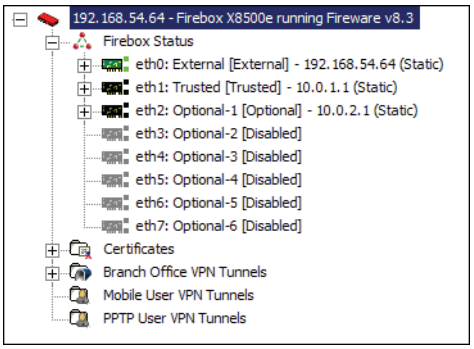
The **Device Management** tab shows management servers connected directly to Watchguard System Manager and the devices connected to those servers. A device managed by the Management Server can also appear on the **Device Status** tab if it is also connected directly to Watchguard System Manager.

The WatchGuard System Manager window also has menus and icons you can use to start other tools.



Device status

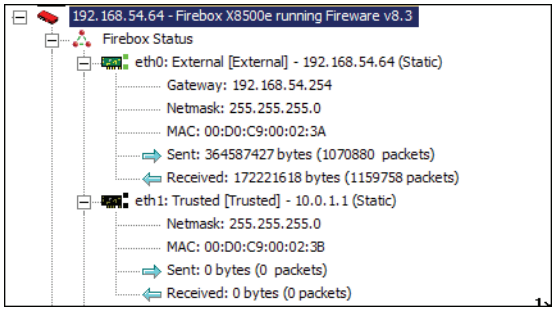
Information about a device you connect to appears in the WatchGuard® System Manager **Device Status** tab.



Firebox Status

Expanded information on a Firebox includes the IP address and subnet mask of each Firebox interface. Expanded information for an interface includes:

- IP address and netmask of the default gateway (for external interface only).



- Media Access Control (MAC) address of the interface.
- Number of packets sent and received on each interface since the last Firebox restart.

Branch Office VPN Tunnels

Below the Firebox Status is a section on branch office virtual private network (BOVPN) tunnels. There are two types of IPSec BOVPN tunnels: VPN tunnels built manually using Policy Manager and VPN tunnels built using the Management Server.

An expanded entry for a BOVPN tunnel shows this information:

- The tunnel name, the IP address of the destination IPSec device, and the tunnel type. If the tunnel is managed by the Management Server, the IP address refers to the full remote network address.
- The volume of data sent and received on the tunnel in bytes and packets.
- The time before the key expires and when the tunnel is created again. This appears as a time limit or as the number of bytes. If you use the Management Server to configure a tunnel to expire using time and volume limits, the two expiration values appear.
- Authentication and encryption layers set for the tunnel.
- Routing policies for the tunnel.

Mobile User VPN tunnels

After the branch office VPN tunnels entry is an entry for Mobile User VPN tunnels. This entry shows the same information as for Branch Office VPN tunnels. It includes the tunnel name, the destination IP address, and the tunnel type. Packet information, the key expiration date, authentication, and encryption data also appear.

PPTP VPN tunnels

For PPTP RUVPN tunnels, WatchGuard System Manager shows only the quantity of sent and received packets. The volume of bytes and total volume of bytes are not applicable to PPTP tunnels.

Connection status

The tree view for each device shows one of four possible states. The status descriptions are as follows:

No exclamation point and gray icon
: The device is being contacted for the first time or has not been contacted yet.

Normal icon
: Usual operation. The device is successfully sending data to WatchGuard System Manager.

Yellow question mark
The device has a dynamic IP address and has not yet contacted the Management Server.

Red exclamation point and gray icon
WatchGuard System Manager cannot make a network connection to the device at this time.

CHAPTER 2

Getting Started

Historically, organizations used many tools, systems, and personnel to control the security of their networks. Different computer systems controlled access, authentication, virtual private networking, and network control. These expensive systems are not easy to use together or to keep up-to-date. WatchGuard® System Manager (WSM) supplies an integrated solution to manage your network and control security problems. This chapter tells you how to install WatchGuard System Manager into your network.

Installing WatchGuard System Manager

WatchGuard® System Manager (WSM) includes firewall appliance software and management software. Use the WSM software to configure and monitor the Firebox®.

To install the WatchGuard System Manager software, you must:

- Collect your network addresses and information
- Select a network configuration mode.
- Select to install the Management Server, Log Server, and WebBlocker Server on the same computer as your management software, or on a different computer.
- Configure the management station
- Use a Quick Setup Wizard to make a basic configuration file
- Put the Firebox into operation on your network

Note

This chapter gives the default information for a Firebox with a three-interface configuration. If your Firebox has more than three interfaces, use the configuration tools and procedures in the "Network Configuration" chapter.

Installation requirements

Before you install WatchGuard System Manager, make sure that you have these items:

- WatchGuard Firebox security device
- A serial cable (blue)

- Three crossover Ethernet cables (red)
- Three straight Ethernet cables (green)
- Power cable
- LiveSecurity Service license key

Collecting network information

License keys

Collect your license key certificates. Your WatchGuard Firebox comes with a LiveSecurity license key that enables the features on your Firebox.

You get the license keys for any optional products when you purchase them.

Network addresses

We recommend that you make two tables when you configure your Firebox. Use the first table for your network IP addresses before you put the Firebox into operation.

WatchGuard uses slash notation to show the subnet mask.

Network IP Addresses Without the Firebox

Wide Area Network	_____._____._____._____ / ____
Default Gateway	_____._____._____._____
Local Area Network	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____
Public Server(s) (if applicable)	_____._____._____._____
	_____._____._____._____
	_____._____._____._____

Use the second table for your network IP addresses after you put the Firebox into operation.

External interface
: Connects to the external network (typically the Internet) that is not trusted.

Trusted interface
: Connects to the private LAN (local area network) or internal network that you want to secure.

Optional interface(s)

Usually connects to the DMZ or the mixed trust area of your network. The number of optional interfaces on your Firebox changes with the model you have purchased. Use optional interfaces to create zones in the network with different levels of access.

Network IP Address With the Firebox

Default Gateway	_____._____._____._____
External Network	_____._____._____._____ / ____
Trusted Network	_____._____._____._____ / ____
Optional Network	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____

Selecting a firewall configuration mode

You must decide how to install the Firebox into your network before you install WatchGuard System Manager. How you install the Firebox controls the interface configuration. To install the Firebox into your network, select the configuration mode—routed or drop-in—that matches the needs of your current network.

Many networks operate best with a routed configuration, but we recommend the drop-in mode if:

- You have already assigned a large number of static IP addresses
- You cannot configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses

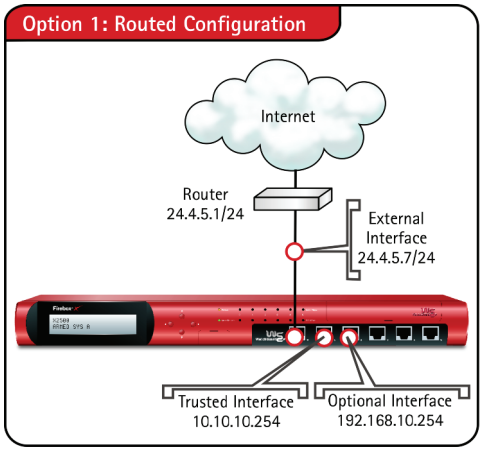
This table and the descriptions below the table show three conditions that can help you to select a firewall configuration mode.

Routed Configuration	Drop-in Configuration
All interfaces of the Firebox are on different networks.	All interfaces of the Firebox are on the same network and have the same IP address.
Trusted and optional interfaces must be on different networks. Each interface has an IP address on its network.	The computers on the trusted or optional interfaces can have a public IP address.
Use static NAT (network address translation) to map public addresses to private addresses behind the trusted or optional interfaces.	The machines that have public access have public IP addresses. Thus, no static NAT is necessary.

Routed configuration

Use the routed configuration when you have a small number of public IP addresses or when your Firebox gets its external IP address with PPPoE (point-to-point protocol over Ethernet) or DHCP (dynamic host configuration protocol).

In a routed configuration, you install the Firebox with different subnets on each of its interfaces. The public servers behind the Firebox can use private IP addresses. The Firebox uses NAT to route traffic from the external network to the public servers.



The requirements for a routed configuration are:

- All interfaces of the Firebox must be configured on different subnets. The minimum configuration includes the external and trusted interfaces. You also can configure one or more optional interfaces.
- All computers connected to the trusted and optional interfaces must have an IP address from that network. For example, a computer on a trusted interface in the previous figure could have an IP address of 10.10.10.200 but not 192.168.10.200, which is on the optional interface.

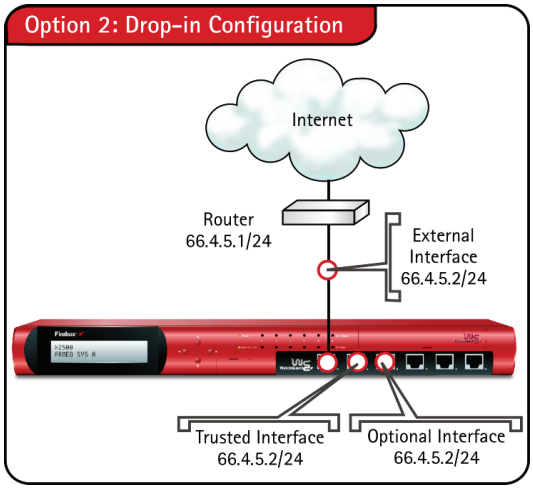
Drop-in configuration

In a drop-in configuration, the Firebox is configured with the same IP address on all interfaces. The drop-in configuration mode distributes the network's logical address range across the Firebox interfaces. You can put the Firebox between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as drop-in because the Firebox is "dropped in" to a network.

In drop-in mode:

- You must assign the same primary IP address to all interfaces on your Firebox (external, trusted, and optional).
- You can assign secondary networks on any interface.
- You can keep the same IP addresses and default gateways for hosts on your trusted and optional networks, and add a secondary network address to the Firebox interface so the Firebox can correctly send traffic to the hosts on these networks.

The public servers behind the Firebox can continue to use public IP addresses. The Firebox does not use network address translation to route traffic from outside your network to your public servers.



The properties of a drop-in configuration are:

- You must have a static external IP address to assign to the Firebox.
- You use one logical network for all interfaces.
- Drop-in mode does not support multi-WAN in round robin or backup order. For more information on these options, see the "Network Setup and Configuration" chapter.

It is sometimes necessary to flush the ARP cache of each computer on the trusted network, but this is not common.

Selecting where to install server software

During installation, you can install the management station and three WatchGuard System Manager server components on the same computer. Or you can use the same installation procedure to install the Log Server and WebBlocker Server components on other computers to distribute server load or supply redundancy. The Management Server does not operate correctly on a computer that does not also have WSM software installed. To decide where to install server software, you must examine the capacity of your management station and select the installation method that matches your needs.

If you install the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their desktop firewall configuration because the installation program opens the necessary ports through Windows Firewall automatically. See "Installing WatchGuard Servers on computers with desktop firewalls" on page 20 for more information.

Setting up the management station

You install WatchGuard System Manager (WSM) software on your management station. This software shows the traffic through the firewall. WatchGuard System Manager also shows connection and tunnel status. The WatchGuard Log Server records information it receives from the Firebox. You can get access to this data using tools on the management station.

Select one computer on your network as the management station and install the management software. To install the WatchGuard System Manager software on your Windows-based management sta-

tion, you must have administrative privileges. After installation, you can operate with Windows XP or Windows 2003 Power User privileges.

You can download the most current WatchGuard System Manager software at any time from https://www.watchguard.com/archive/softwarecenter.asp. You must log in with your LiveSecurity user name and password. If you are a new user, create a user profile and activate your product at http://www.watchguard.com/activate before you try to download the WSM software.

1 Download the latest WatchGuard System Manager software. You must also download and install the latest Fireware® appliance software to your management station. You use this software with the Web Quick Setup Wizard to create a basic configuration file for your Firebox.
   Make sure that you write down the name and the path of the files when you save them to your hard drive.
2 Open the file and use the installation instructions.
   The Setup program includes a screen in which you select the components of the software or the upgrades to install. A different license is necessary when you install some software components.

Note

If your management station is operating with a Windows toolbar, some users find it necessary to close and restart the toolbar to see the new components installed for the WatchGuard Management System.

Software encryption levels

The management station software is available in two encryption levels.

Base

Supports 40-bit encryption for PPTP RUVPN tunnels. You cannot create an IPSec VPN tunnel with this level of encryption.

Strong

Supports 40-bit and 128-bit encryption for PPTP RUVPN. Also supports 56-bit and 168-bit DES, and 128-bit, 192-bit, and 256-bit AES.

To use virtual private networking with IPSec you must download the strong encryption software.

Strong export limits apply to the strong encryption software. It is possible that it is not available for download.

Backing up your previous configuration

If you have a previous version of WatchGuard System Manager, make a backup of your security policy configuration before you install a new version. To create a backup of your configuration, see the *WatchGuard® WFS to Fireware Migration Guide*.

Quick Setup Wizard

You can use a Quick Setup Wizard to create a basic configuration for your Firebox X. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall. You can use this same procedure any time you want to reset the Firebox to a new basic configuration for recovery or other reasons.

Firebox X Core and Peak e-Series Web Quick Setup Wizard

When you purchase a Firebox X Core or Peak e-Series device, you can use the new Web Quick Setup Wizard to configure your Firebox. If you have configured a Firebox X Core or X Peak before, it is important for you to understand that the Web Quick Setup Wizard operates differently than the Quick Setup Wizard that shipped with earlier Firebox X hardware models. With earlier Firebox X Core and Peak devices, the Quick Setup Wizard used device discovery to find a Firebox on the network to configure. With the Firebox X Core and Peak e-Series and the Web Quick Setup Wizard, you must make a direct network connection to the Firebox and use a web browser to start the wizard. The Firebox uses DHCP from its Eth1 Ethernet interface to give a new IP address to your management station to use during configuration.

Before you start the Web Quick Setup Wizard, make sure you have:

- Registered your Firebox with LiveSecurity Service
- Stored a copy of your Firebox feature key in a text file on your management station
- Downloaded WSM and Fireware® software from the LiveSecurity Service web site to your management station
- Installed the Fireware executable on your management station
- Configured your management station to accept an IP address automatically (through DHCP)

Using the Web Quick Setup Wizard

1 Connect the red cross-over Ethernet cable that ships with your Firebox between the Ethernet port on your management station and the Eth1 port on your Firebox.

2 Plug the power cord into the Firebox power input and into a power source.

3 On the front of the Firebox X, press the up arrow button while you turn on the power to the Firebox.
The Firebox X boots into Safe Mode. You can release the up arrow button when you see the message "Invoking Recovery".

4 Make sure your management station is configured to accept DHCP-assigned IP addresses.
For example, if your management station uses Windows XP:
From your Windows Start menu, select **All Programs > Control Panel > Network Connections > Local Area Connections**. Click **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Make sure **Obtain an IP Address Automatically** is selected.

5 Open a web browser and type: **http://10.0.1.1:8080/**
This opens an HTTP connection between your management station and the Firebox X e-Series device. The Web Quick Setup Wizard starts automatically.

After the Firebox is configured with this basic configuration, you can use Policy Manager to expand or change the Firebox configuration.

Using Web Quick Setup Wizard for recovery

You can use the Web Quick Setup Wizard when you first configure your Firebox X e-Series device. You can also use the Web Quick Setup Wizard if you want to reset a Firebox with a new configuration because you forgot the password or because the Firebox is deploying in a new network.

If you use the Web Quick Setup Wizard for recovery and you have purchased a Firebox hardware model upgrade, you must make sure that the feature key you put in the wizard is the feature key that you received with the model upgrade.

Troubleshooting problems with the Web Quick Setup Wizard

If the Web Quick Setup Wizard is unable to install Fireware appliance software on the Firebox, the wizard times out after six minutes. Here are some things to check if you have problems with the wizard:

- It is possible that the Fireware application software file you downloaded from the LiveSecurity web site is corrupted. If the software image is corrupted, you can sometimes see a message on the LCD interface: "File Truncate Error." Download the software again and try the wizard once more.
- If you use Internet Explorer 6, clear the file cache in your web browser and try again. To clear the cache, from the Internet Explorer toolbar select **Tools > Internet Options > Delete Files**.

Quick Setup Wizard

If you use an older model Firebox X Core or Peak (not an e-Series Firebox), then you must use the Quick Setup Wizard that runs as a Windows application to make a basic configuration file. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall.

After the Firebox is configured with this basic configuration, you can use Policy Manager to expand or change the Firebox configuration.

The Quick Setup Wizard uses a device discovery procedure to find the Firebox X model you are configuring. This procedure uses a UDP broadcast. Software firewalls, including the firewall in Microsoft Windows XP SP2, can cause problems with device discovery.

You can start the Quick Setup Wizard from the Windows desktop or from WatchGuard System Manager. From the desktop, select **Start > All Programs > WatchGuard System Manager 8.3 > Quick Setup Wizard**. From System Manager, select **Tools > Quick Setup Wizard**.

Note

In the Quick Setup Wizard, you must set a status and configuration passphrase for the Firebox. When you are ready to configure a Log Server to collect log messages from the Firebox, use the status passphrase you set in the Quick Setup Wizard as your default log encryption key. After your Log Server is configured, you can change your log encryption key if you want. For more information, see the "Logging and Notification" chapter.

Putting the Firebox into Operation

When you finish with either Quick Setup Wizard, you have completed the installation of your Firebox®. You can use the Firebox as a basic firewall that allows all outgoing TCP, DNS, and ping traffic.

Complete these steps to put the Firebox into operation on your network:

- Put the Firebox in its permanent physical location.
- In WatchGuard® System Manager, use **File > Connect To Device** to connect the management station to the Firebox.
- If you use a routed configuration, change the default gateway on all computers that you connect to the Firebox trusted IP address.
- Set up the Management Server. See the "Management Server Setup and Administration" chapter in this guide.
- Configure the Log Server to start recording log messages. See the "Logging and Notification" chapter in this guide.
- Set up the WebBlocker Server. See the "Controlling Web Site Access with WebBlocker" chapter in this guide.
- Open Policy Manager to change the configuration.

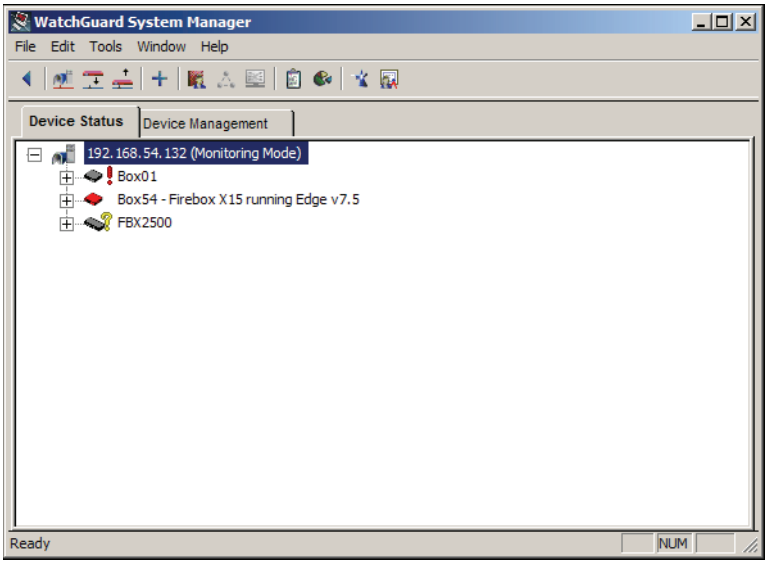
Note

If you install the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See the section "Installing WatchGuard Servers on computers with desktop firewalls" on page 20 for more information.

Starting WatchGuard System Manager

This section provides basic procedures to get you started using WatchGuard System Manager. It also describes the information you see on the screen when you first connect to a Firebox.

From the Windows Desktop, select **Start > All Programs > WatchGuard System Manager 8.3 > WatchGuard System Manager**.



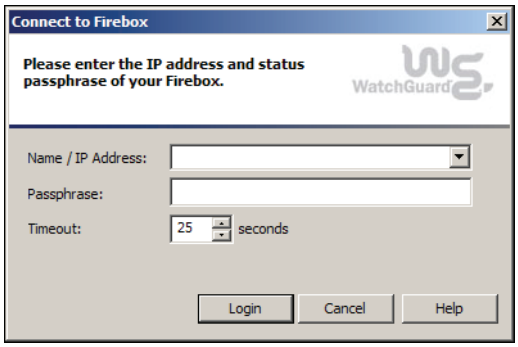
For basic information on WatchGuard System Manager, see "WatchGuard System Manager (WSM) User Interface" on page 4. You can get access to all WatchGuard System Manager functionality through this main window, as described throughout this manual.

Connecting to a Firebox

1 Select **File > Connect to > Device**.
or
Right-click in the **Device Status** tab and select **Connect to > Device**.

or
Click the Connect to Device icon on the WatchGuard® System Manager toolbar. The icon is shown at left.

The **Connect to Device** dialog box appears.



2 From the **Firebox** drop-down list, select a Firebox® by its IP address or host name.
You can also type the IP address or host name. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

3 Type the Firebox status (read-only) passphrase.
You use the status passphrase to monitor traffic and Firebox conditions. You must type the configuration passphrase when you save a new configuration to the Firebox.

4 If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Firebox, before it sends a message that shows that it cannot get data from the device.
If you have a slow network or Internet connection to the device, you can increase the time-out value. Decreasing the value decreases the time you must wait for a time-out message if you try to connect to a Firebox that is not available.

5 Click **Login**.
The Firebox appears in the WatchGuard System Manager window.

Disconnecting from a Firebox

To disconnect, right-click the first line of information for the Firebox to disconnect from and select **File > Disconnect**. Or select the Firebox and then click the Disconnect icon shown at left.

Starting security applications

You can start these tools from WatchGuard® System Manager using the icons on the taskbar and menu options:

Policy Manager

Policy Manager lets you install, configure, and customize a network security policy. To configure or customize the security policy of a Firebox® X Edge or Firebox SOHO, you must use the web user interface to connect to the device.

Firebox System Manager

WatchGuard Firebox System Manager lets you start many different security tools in one easy to user interface. You also can use Firebox System Manager to monitor real-time traffic through the firewall. For information on using Firebox System Manager, see the “Monitoring Firebox Status” chapter.

HostWatch

HostWatch shows the connections through a Firebox from the trusted network to the external network. It shows the current connections, or it can show historical connections from a log file. For information on using HostWatch, see the “Monitoring Firebox Status” chapter.

Log Viewer

Log Viewer shows a static view of a log file. It lets you:

- Apply a filter by data type
- Search for words and fields
- Print and save to a file

For more information on using Log Viewer, see the "Logging and Notification" chapter in this guide.

Historical Reports

These HTML reports give data to use when you monitor or troubleshoot the network. The data can include:

- Type of session
- Most active hosts
- Most used services
- URLs

For information on using Historical Reports, see the chapter "Generating Reports of Network Activity" in this guide.

After Your Installation

You have satisfactorily installed, configured, and put your new WatchGuard® System Manager into operation on your network. Here are some basic procedures and some more information to think about.

Customizing your security policy

Your security policy controls who can get in to your network, where they can go, and who can get out. The configuration file of your Firebox® makes the security policy.

The configuration file that you make with the Quick Setup Wizard is only a basic configuration. You can make a configuration file that aligns your security policy with your requirements. To do this, add filtered and proxied policies to set what you let in and out of your network. Each policy can have an effect on your network. The policies that increase your network security can decrease access to your network. The policies that increase access to your network can decrease your network security. When you select these policies, you must select a range of balanced policies based on your organization and the computer equipment that you protect. For a new installation, we recommend that you use only packet filter policies until all your systems operate correctly. As necessary, you can add proxied policies.

Features of the LiveSecurity Service

Your Firebox includes a subscription to LiveSecurity® Service. Your subscription:

- Makes sure that you get the newest network protection with the newest software upgrades
- Gives solutions to your problems with full technical support resources
- Prevents service interruptions with messages and configuration help for the newest security problems
- Helps you to find out more about network security through training resources
- Extends your network security with software and other features
- Extends your hardware warranty with advanced replacement

Upgrading to a New Version of Fireware

Occasionally, we make new versions of WatchGuard System Manager (WSM) and Fireware® appliance software available to Firebox® users with active LiveSecurity subscriptions. To upgrade from one version of WSM 8.x with Fireware to a new version of WSM 8.x with Fireware:

1 Back up your current Firebox configuration file and Management Server configuration files

For more information on how to create a backup image of your Firebox configuration, see "About Firebox Backup Images" on page 72.

To back up the settings on your Management Server, use the Management Server Backup and Restore Wizard. For more information on this wizard, see the "Management Server Setup and Administration" chapter.

2 Use Windows Add or Remove Programs to uninstall your existing WatchGuard Fireware installation.

It is not necessary to remove the WSM installation.

3 Launch the file or files that you downloaded from the LiveSecurity web site and use the on-screen procedure.

4 To save the upgrade to the appliance, use Policy Manager to open your Firebox X Core or Firebox X Peak configuration file and use the on-screen instructions to convert the configuration file to the newer version and save it to the Firebox.

If you do not see on-screen instructions or have problems with this procedure, open Policy Manager and select **File > Upgrade**. Browse to your installation directory or C:\Program Files\Common Files\WatchGuard\resources\Fireware and select the WGU file. Click **OK**.

The upgrade procedure automatically restarts the Firebox.

Installation Topics

This section gives additional information about setting up your Firebox®.

Installing WatchGuard Servers on computers with desktop firewalls

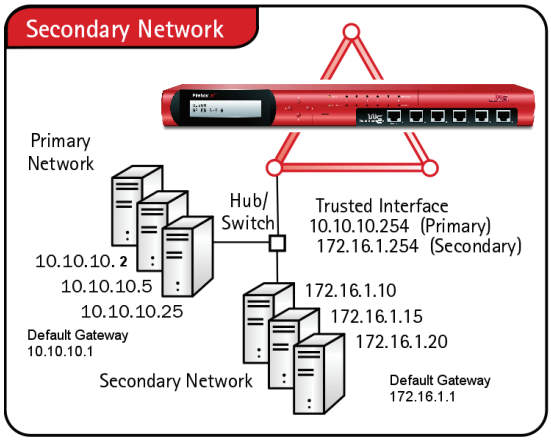
Desktop firewalls can block the ports necessary for WatchGuard® server components to operate. Before you install the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall, you might need to open the necessary ports on the desktop firewall. Windows Firewall users do not need to change their configuration because the installation program opens the necessary ports in Windows Firewall automatically.

This table shows you the ports you must open on a desktop firewall.

Server Type/Appliance Software	Protocol/Port
Management Server	TCP 4109, TCP 4110, TCP 4112, TCP 4113
Log Server with Fireware® appliance software with WFS appliance software	 TCP 4115 TCP 4107
WebBlocker Server	TCP 5003, UDP 5003

Adding secondary networks to your configuration

A secondary network is a different network that connects to a Firebox interface with a switch or hub.



When you add a secondary network, you map a second IP address to the Firebox interface. Thus, you make (or add) an IP alias to the network interface. This secondary network address you set is the default gateway for all the computers on the secondary network. The secondary network also tells the Firebox that there is one more network on the Firebox interface.

To add a secondary network, do one of these procedures:

Use a Quick Setup Wizard during installation

If you configure the Firebox in drop-in mode, you can enter an IP address for the secondary network in the Web Quick Setup Wizard. This is the default gateway for your secondary private network.

Add the secondary network after the Firebox installation is complete

If you configure the Firebox in routed mode, or at any time after you use a Quick Setup Wizard, you can use Policy Manager to add secondary networks to an interface. For information on how to use Policy Manager, see the "Configuring Policies" chapter in this guide.

Dynamic IP support on the external interface

If you use dynamic IP addresses, you must configure your Firebox in routed mode when you use a Quick Setup Wizard.

If you select DHCP, the Firebox tells a DHCP server controlled by your Internet service provider (ISP) to give the Firebox its IP address, gateway, and netmask. This server can also give DNS server information for your Firebox. If it does not give you that information, you must add it manually to your configuration. If necessary, you can change the IP addresses that your ISP gives you.

You also can use PPPoE. As with DHCP, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and netmask.

If you use PPPoE on the external interface, you must have the PPP user name and password when you configure your network. If your ISP gives you a domain name to use, type your user name in the format "user@domain" when you use a Quick Setup Wizard.

A static IP address is necessary for the Firebox to use some functions. When you configure the Firebox to receive dynamic IP addresses, the Firebox cannot use these functions:

- High Availability (not available on Firebox 500)
- Drop-in mode
- 1-to-1 NAT
- MUVPN
- RUVPN with PPTP

Note

If your ISP uses a PPPoE connection to give a static IP address, the Firebox allows you to enable MUVPN and RUVPN with PPTP because the IP address is static.

External aliases and 1-to-1 NAT are not available when the Firebox is a PPPoE client.

Entering IP addresses

When you enter IP addresses in a Quick Setup Wizard or WSM dialog boxes, type the digits and periods in the correct sequence. Do not use the TAB key, arrow key, spacebar, or mouse to put your cursor after the periods. For example, if you type the IP address 172.16.1.10, do not type a space after you type "16." Do not try to put your cursor after the subsequent period to type "1." Type a period directly after "16," and then type "1.10." Press the slash (/) key to move to the netmask.

About slash notation

Use slash notation to enter the netmask. In slash notation, one number shows how many bits of the IP address identify the network that the host is on. A netmask of 255.255.255.0 has a slash equivalent of 8+8+8=24. For example, an IP address 192.168.42.23/24 is equivalent to an IP address of 192.168.42.23 with a netmask of 255.255.255.0.

This table shows the network masks and their slash equivalents:

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Installing the Firebox cables

Connect the power cable to the Firebox power input and to a power source.

We recommend that you use a straight Ethernet cable (green) to connect your management station to a hub or switch. Use a different straight Ethernet cable (green) to connect your Firebox to the same hub or switch.

You also can use a red crossover cable to connect the Firebox trusted interface to the management station Ethernet port.

CHAPTER 3

Service and Support

No Internet security solution is complete without regular updates and security information. New threats appear each day — from the newest hacker to the newest bug in an operating system — and each can cause damage to your network systems. LiveSecurity® Service sends security solutions directly to you to keep your security system in the best condition. Training and technical support are available on the WatchGuard® site to help you learn more about network security and your WatchGuard products.

LiveSecurity Service Solutions

The number of new security problems and the volume of information about network security continues to increase. We know that a firewall is only the first component in a full security solution. The WatchGuard® Rapid Response Team is a dedicated group of network security personnel who can help you to control the problem of too much security information. They monitor the Internet security web sites to identify new security problems.

Threat responses, alerts, and expert advice

After a new threat is identified, the WatchGuard Rapid Response Team sends you an e-mail to tell you about the problem. Each message gives full information about the type of security problem and the procedure you must use to make sure that your network is safe from attack.

Easy software updates

LiveSecurity® Service saves you time because you receive an e-mail when we release a new version of the WatchGuard System Manager software. Installation wizards, release notes, and a link to the software update make for a fast and easy installation. These continued updates make sure that you do not have to use your time to find new software.

Access to technical support and training

You can find information about your WatchGuard products quickly with our many online resources. You can also speak directly to one of the WatchGuard technical support personnel. Use our online training to

learn more about the WatchGuard System Manager software, Firebox®, and network security, or find a WatchGuard Certified Training Center in your area.

LiveSecurity Service Broadcasts

The WatchGuard® Rapid Response Team regularly sends messages and software information directly to your computer desktop by e-mail. We divide the messages into categories to help you to identify and make use of incoming information immediately.

Information Alert

Information Alerts give you a fast view of the newest information and threats to Internet security. The WatchGuard Rapid Response Team frequently recommends that you make a security policy change to protect against the new threat. When necessary, the Information Alert includes instructions on the procedure.

Threat Response

If a new security threat makes it necessary, the WatchGuard Rapid Response Team transmits a software update for your Firebox®. The Threat Response includes information about the security threat and instructions on how to download a software update and install it on your Firebox and management station.

Software Update

When necessary, WatchGuard updates the WatchGuard System Manager software. Product upgrades can include new features and patches. When we release a software update, you get an e-mail with instructions on how to download and install your upgrade.

Editorial

Each week, top network security personnel come together with the WatchGuard Rapid Response Team to write about network security. This continuous supply of information can help your network be safe and secure.

Foundations

The WatchGuard Rapid Response Team also writes information specially for security administrators, employees, and other personnel that are new to this technology.

Loopback

At the end of each month LiveSecurity® Service sends you an e-mail with a summary of the information sent that month.

Support Flash

These short training messages can help you to operate WatchGuard System Manager. They are an added resource to the other online resources:

- Online Help
- FAQs
- Known Issues pages on the Technical Support web site

Virus Alert

WatchGuard has come together with antivirus vendor McAfee to give you the most current information about computer viruses. Each week, we send you a message with a summary of the virus traffic on the Internet. When a hacker releases a dangerous virus on the Internet, we send a special virus alert to help you protect your network.

New from WatchGuard

When WatchGuard releases a new product, we first tell you — our customers. You can learn about new features and services, product upgrades, hardware releases, and promotions.

Activating LiveSecurity Service

You can activate LiveSecurity® Service through the activation section of the LiveSecurity web pages. There is information about feature activation and the Quick Setup Wizard in the *Quick Start Guide* and in the "Getting Started" chapter of this book.

Note

To activate LiveSecurity Service, you must enable JavaScript on your browser.

To activate LiveSecurity Service through the Internet:

1 Make sure that you have your Firebox® serial number. This is necessary during the LiveSecurity activation procedure.
   - You can find the Firebox serial number on a label on the rear side of the Firebox below the Universal Product Code (UPC), or on a label on the bottom of the Firebox.
   - The license key number is on the WatchGuard LiveSecurity License Key certificate. Make sure that you enter the license key in all capital letters and include hyphens.

2 Use your web browser to go to:
www.watchguard.com/account/register.asp
The Account page appears.

3 Complete the LiveSecurity Activation page. Use the TAB key or the mouse to move through the fields on the page.
You must complete all the fields to activate correctly. This information helps WatchGuard to send you the information and software updates that are applicable to your products.

4 Make sure that your e-mail address is correct. Your LiveSecurity e-mails about product updates and threat responses come to this address. After you complete the procedure, you get an e-mail message that tells you that you activated LiveSecurity Service satisfactorily.

5 Click **Register**.

LiveSecurity Service Self Help Tools

Online Self Help Tools enable you to get the best performance from your WatchGuard® products.

Note

You must activate LiveSecurity® Service before you can access online resources.

Instant Answers

Instant Answers is a guided Help tool designed to give solutions to product questions very quickly. Instant Answers asks you questions and then gives you to the best solution based on the answers you give.

Basi*c FAQs*

The Basic FAQs (frequently asked questions) give you general information about the Firebox® and the WatchGuard System Manager software. They are written for the customer who is new to network security and to WatchGuard products.

Advanced FAQs

The Advanced FAQs (frequently asked questions) give you important information about configuration options and operation of systems or products. They add to the information you can find in this User Guide and in the Online Help system.

Fireware® "How To"'s

The Fireware How To documentation helps you to quickly find procedures for configuration tasks specific to Fireware appliance software.

Known Issues

This Known Issues tool monitors WatchGuard product problems and software updates.

WatchGuard Users Forum

The WatchGuard Technical Support team operates a web site where customers can help each other with WatchGuard products. Technical Support monitors this forum to make sure you get accurate information.

Online Training

Browse to the online training section to learn more about network security and WatchGuard products. You can read training materials and get a certification in WatchGuard products. The training includes links to a wide range of documents and web sites about network security. The training is divided into parts, which lets you use only the materials you feel necessary. To learn more about online training, browse to:
www.watchguard.com/training/courses_online.asp

Learn About

Learn About is a list of all resources available for a specified product or feature. It is a site map for the feature.

Product Documentation

The WatchGuard web site has a copy of each product user guide, including user guides for software versions that are no longer supported. The user guides are in .pdf format.

General Firebox X Edge and Firebox SOHO Resources

This section of the web site shows basic information and links for Firebox X Edge and Firebox SOHO customers. It can help you to install and use the Firebox X Edge and SOHO hardware.

To get access to the LiveSecurity Service Self Help Tools:

1 Start your web browser. In the address bar, type:
http://www.watchguard.com/support

2 Click **Self Help Tools**.
You must log in.

3 Click your selection.

WatchGuard Users Forum

The WatchGuard® Users Forum is an online group. It lets users of WatchGuard products interchange product information about:

- Configuration
- Connecting WatchGuard products and those of other companies
- Network policies

This forum has different categories that you can use to look for information. The Technical Support team controls the forum during regular work hours. You do not get special help from Technical Support when you use the forum. To contact Technical Support directly from the web, log in to your LiveSecurity account. Click on the **Incidents** link to send a Technical Support incident.

Using the WatchGuard Users Forum

To use the WatchGuard Users Forum you must first create an account. Browse to http://www.watchguard.com/forum for instructions.

Online Help

WatchGuard® online Help is a web system that can operate on most computer operating systems. We release each version of the software products with a full online Help system.

A static version of Help is installed automatically with the WatchGuard System Manager software. You can find it in a subdirectory of the installation folder with the name Help.

Starting WatchGuard online Help

To start the online Help system from the WatchGuard System Manager software, press **F1**. Your browser opens and an online Help page appears. The page has information about the feature you are using.

Searching for information

There are three methods to search for information in the WatchGuard online Help system:

Contents
: The **Contents** tab shows a list of categories in the Help system. Double-click a book to expand a category. Click a page title to look at the contents of that category.

Index
: The index shows a list of the words that are in the Help system. Type the word, and the list automatically goes to those words that start with the typed letters. Click a page title to look at the contents.

Search
: The search feature is a full text search of the Help system. Type a word and press ENTER. A list shows the categories that contain the word. The search feature does not operate with AND, OR, or NOT operators.

Copy the online Help system to more computers

You can copy WatchGuard online Help from the management station to a second computer. When you do this, copy the full online Help folder from the WatchGuard installation directory on the management station. You must include all subdirectories.

Software requirements

- Internet Explorer 4.0 or a subsequent version

- Netscape Navigator 4.7 or a subsequent version

Operating system

- Windows NT 4.0, Windows 2000, or Windows XP
- Sun Solaris
- Linux

Product Documentation

We copy all user guides to the web site at http://www.watchguard.com/help/documentation.

Technical Support

Your LiveSecurity® Service subscription includes technical support for the WatchGuard® System Manager software and Firebox® hardware. To learn more about WatchGuard Technical Support, browse to the WatchGuard web site at:

http://www.watchguard.com/support

Note

You must activate LiveSecurity Service before you can get technical support.

LiveSecurity Service technical support

All new Firebox products include the WatchGuard LiveSecurity Technical Support Service. You can speak with a member of the WatchGuard Technical Support team when you have a problem with the installation, management, or configuration of your Firebox.

Hours

WatchGuard LiveSecurity Technical Support operates from 6:00 AM to 6:00 PM in your local time zone, Monday through Friday.

Telephone number

877.232.3531 (select option #2) in United States and Canada
+1.206.613.0456 in all other countries

Web site

http://www.watchguard.com/support

Service time

We try for a maximum response time of four hours.

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After Hours Upgrade (SIAU) are also available. For more data about these upgrades, refer to the WatchGuard web site at:

http://www.watchguard.com/support

LiveSecurity Gold

WatchGuard Gold LiveSecurity Technical Support adds to your standard LiveSecurity Service. We recommend that you get this upgrade if you use the Internet or VPN tunnels for most of your work.

With WatchGuard Gold LiveSecurity Technical Support you get:

- Technical support 24 hours a day, seven days a week, including holidays.
- The Technical Support Team operates the support center from 7 PM Sunday to 7 PM Friday (Pacific Time). For weekend support for critical problems, use the on-call paging system.
- We try for a maximum response time of one hour.
- To create a support incident, call WatchGuard LiveSecurity Technical Support. A Customer Care representative records the problem and gives you an incident number. A Priority Support technician calls you as quickly as possible. If you have a critical problem when the support center is not open, use the LiveSecurity Technical Support phone number to page a technician. You can also send an incident on the web site at: http://www.watchguard.com/support/incidents/newincident.asp.

Firebox Installation Service

WatchGuard Remote Firebox Installation Service helps you to install and configure your Firebox. You can schedule two hours with a WatchGuard Technical Support team member. The technician helps you to:

- Do an analysis of your network and security policy
- Install the WatchGuard System Manager software and Firebox hardware
- Align your configuration with your company security policy

This service does not include VPN installation.

VPN Installation Service

WatchGuard Remote VPN Installation Service helps you through a full VPN installation. You can schedule a two-hour time with one of the WatchGuard Technical Support team. During this time, the technician helps:

- Do an analysis of your VPN policy
- Configure your VPN tunnels
- Do a test of your VPN configuration

You can use this service after you correctly install and configure your Firebox devices.

Training and Certification

WatchGuard® product training is available online to help you learn more about network security and WatchGuard products. You can find training materials on the Technical Support web site and prepare for a certification exam. The training materials include links to books and web sites with more information about network security.

WatchGuard product training is also available at a location near you through a large group of WatchGuard Certified Training Partners (WCTPs). Training partners give training using certified training materials and with WatchGuard hardware. You can install and configure the products with an advanced instructor and system administrator to help you learn. To find a training partner, go to

http://www.watchguard.com/training/partners_locate.asp

CHAPTER 4

Monitoring Firebox Status

WatchGuard® Firebox® System Manager (FSM) gives you one interface to monitor all components of a Firebox and the work it does. From FSM, you can monitor the current condition of the Firebox, or connect to the Firebox directly to update its configuration. You can see:

- Status of the Firebox interfaces and the traffic that goes through the interfaces
- Status of VPN tunnels and management certificates
- Real-time graphs of Firebox bandwidth use or of the connections on specified ports
- Status of any other security services you use on your Firebox

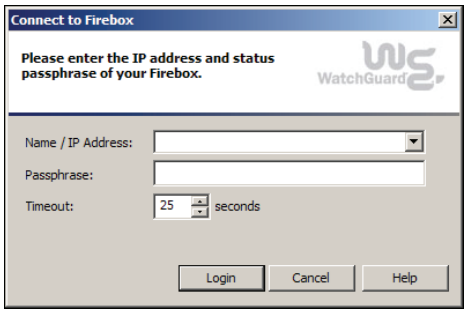
Starting Firebox System Manager

Before you start to use Firebox® System Manager, you must connect to a Firebox.

Connecting to a Firebox

1 From WatchGuard System Manager, click the Connect to Device icon.

Or, you can select File > Connect To Device.
The Connect to Firebox dialog box appears.



2 From the **Name/IP Address** drop-down list, select a Firebox.
You can also type the IP address or name of the Firebox.

3 In the **Passphrase** box, type the Firebox status (read-only) passphrase.

4 Click **Login**.
The Firebox appears in the WatchGuard System Manager window.

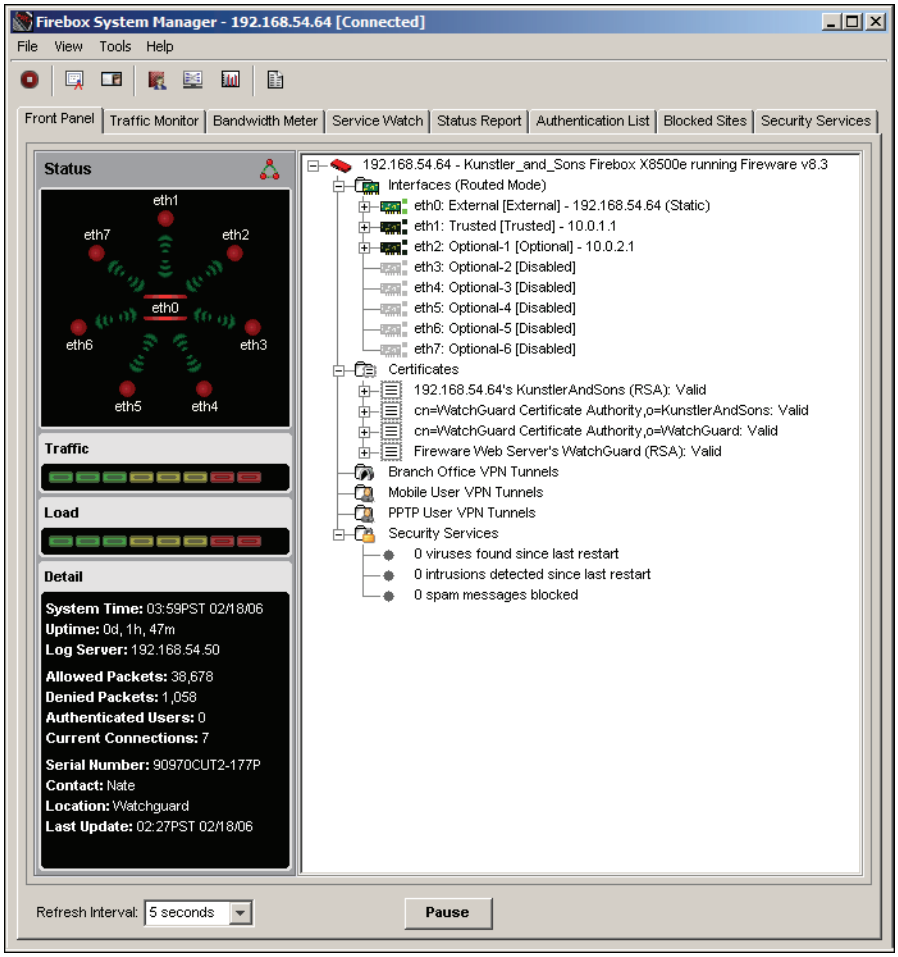
Opening Firebox System Manager

1 From WatchGuard System Manager, select the **Device Status** tab.

2 Select the Firebox to examine with Firebox System Manager.

3 Click the Firebox System Manager icon.

Firebox System Manager appears. Then it connects to the Firebox to get information about the status and configuration.



Firebox System Manager Menus and Toolbar

Firebox® System Manager (FSM) commands are in the menus at the top of the window. The most common tasks are also available as buttons on the toolbar. The tables that follow tell you the function of the menus and toolbar buttons.

Firebox System Manager Menus

Menu	Command	Function
File	Settings	Changes how Firebox System Manager shows status information in the displays.
	Disconnect	Keeps Firebox System Manager open, but stops the connection to the monitored Firebox
	Reset	Stops the operating system components on the Firebox and restarts them (soft reboot)
	Reboot	Starts the current Firebox again.
	Shutdown	Turns off the Firebox.
	Close	Closes the Firebox System Manager window.
VIew	Certificates	Lists the certificates on the Firebox.
	Licenses	Lists the current licenses on the Firebox.
	Communication Log	Opens the communication log, which contains information such as the success or failure of logins, handshakes, and so on. These are connections between the Firebox and Firebox System Manager.
Tools	Policy Manager	Opens Policy Manager with the configuration of the selected Firebox.
	HostWatch	Opens HostWatch connected to the current Firebox.
	Performance Console	Opens the Performance Console, which shows graphs of performance aspects of the Firebox.
	Synchronize Time	Synchronizes the time of the Firebox with the system time.
	Clear ARP Cache	Empties the ARP cache of the selected Firebox.
	Clear Alarm	Empties the alarm list on the selected Firebox.
	High Availability	Configures High Availability options.
	Change Passphrases	Changes the status and configuration passphrases.
Help	Firebox System Manager Help	Opens the online help files for this application.
	About	Shows version and copyright information.

Firebox System Manager Toolbar

Icon	Function
	Starts the display again. This icon appears only when you are not connected to a Firebox.
	Stops the display. This icon appears only when you are connected to a Firebox.
	Shows the management and VPN certificates saved on the Firebox.
	Shows the licenses registered and installed for this Firebox.
	Starts Policy Manager. Use Policy Manager to make or change a configuration file.
	Starts HostWatch, which shows connections for this Firebox.

Icon	Function
	Starts the Performance Console where you can configure graphs that show Firebox status.
	Starts the Communication Log dialog box to show connections between Firebox System Manager and the Firebox.

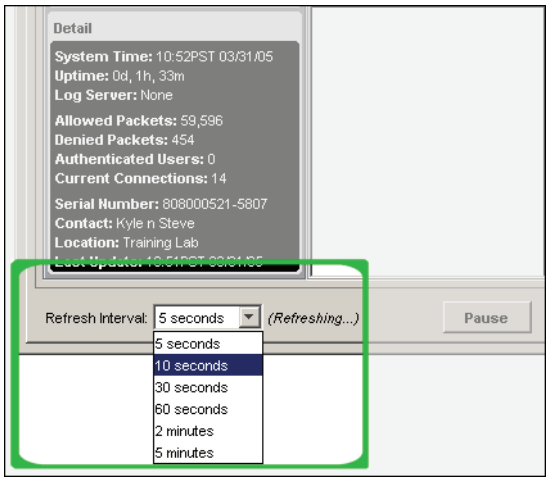
Setting refresh interval and pausing the display

All tabs on Firebox System Manager have, at the bottom of the screen, a drop-down list to set the refresh interval, and a **Pause** button to stop the display:

Refresh Interval

The refresh interval is the polling interval; the time between refreshes of the display. You can change the interval of time (in seconds) that Firebox System Manager gets the Firebox information and sends updates to the user interface.

You must balance how frequently you get information and the load on the Firebox. Be sure to examine the refresh interval on each tab. When a tab gets new information for its display, the text "Refreshing..." appears adjacent to the **Refresh Interval** drop-down list. A shorter time interval gives a more accurate display, but creates more load on the Firebox. From Firebox System Manager, use the **Refresh Interval** drop-down list to select a new duration between window refreshes. You can select 5 seconds, 10 seconds, 30 seconds, 60 seconds, 2 minutes, or 5 minutes. You can also type a custom value into this box.



Pause/Continue

You can click the **Pause** button to temporarily stop Firebox System Manager from refreshing this window. After you click the **Pause** button, this button changes to a **Continue** button. Click **Continue** to continue to refresh the window.

Seeing Basic Firebox and Network Status

The **Front Panel** tab of Firebox® System Manager shows basic information about your Firebox, your network, and network traffic.

Using the Security Traffic display

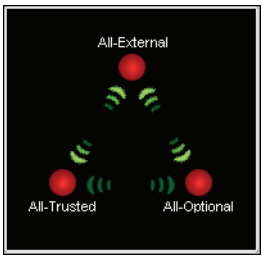
Firebox System Manager initially has a group of indicator lights to show the direction and volume of the traffic between the Firebox interfaces. The display can be a triangle (below left) or a star (below center and right).

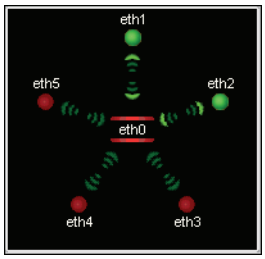
Triangle display

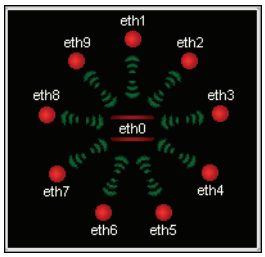
If a Firebox has only three configured interfaces, each corner of the triangle is one interface. If a Firebox has more than three interfaces, each corner of the triangle represents one type of interface. For example, if you have six configured interfaces with one external, one trusted, and four optional interfaces, the "All-Optional" corner in the triangle represents all four of the optional interfaces.

Star display

The star display shows all traffic in and out of the center interface. An arrow that moves from the center interface to a node interface shows that the Firebox is passing traffic. The traffic comes in through the center interface and goes out through the node interface. For example, if eth1 is at the center and eth2 is at a node, a green arrow shows that traffic flows from eth1 to eth2. There are two star displays — one for a Firebox X Core with 6 interfaces and one for Firebox X Peak with 10 interfaces.







To change the display, right-click it and select **Triangle Mode** or **Star Mode**.

Monitoring status information

The points of the star and triangle show the traffic that flows through the interfaces. A green point shows traffic is being allowed at that interface. A red point shows that traffic is being denied, or that the interface is denying some traffic and allowing other traffic. Each point shows incoming connections and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows light up in the direction of the traffic.

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny)—The Firebox denies a connection on that interface.
- Green (allow)—There is traffic between this interface and a different interface (but not the center) of the star. When there is traffic between this interface and the center, the point between these interfaces shows as green arrows.

In the triangle, the network traffic shows in the points of the triangle. The points show only the idle or deny condition. One exception is when there is a large quantity of VPN "tunnel switching" traffic. Tunnel switching traffic refers to packets that are sent through a VPN to a Firebox configured as the default gateway for the VPN network. In this case, the Firebox System Manager traffic level indicator can show very high traffic, but you do not see green lights as more tunnel switching traffic comes in and goes out of the same interface.

Setting the center interface

If you use the star figure, you can customize the interface that appears in its center. Click the interface name or its point. The interface then moves to the center of the star. All the other interfaces move clockwise. If you move an interface to the center of the star, you can see all traffic between that interface and all other interfaces. The default display shows the external interface in the center.

Monitoring traffic, load, and status

Below the **Security Traffic Display** are the traffic volume indicator, processor load indicator, and basic status information (Detail).

The two bar graphs show the traffic volume and the Firebox capacity.

Firebox and VPN tunnel status

The section in Firebox System Manager to the right side of the front panel shows:

- Status of the Firebox
- Certificates
- Branch office VPN tunnels
- Mobile user and PPTP VPN tunnels
- Viruses, intrusions, and spam e-mail messages found

Firebox Status

In the Firebox Status section, expand the entries to see:

- Status of the High Availability feature. When it has a correct configuration and is available, the IP address of the standby Firebox appears. If High Availability is installed, but there is no network connection to the secondary Firebox, a “Not Responding” message appears.
- The IP address of each Firebox interface and the configuration mode of the external interface.
- Status of the CA (root) certificate and the IPSec (client) certificate.

If you again expand the entries in the Firebox System Manager main window, you can see:

- IP address and netmask of each configured interface
- The Media Access Control (MAC) address of each interface
- Number of packets that are sent and received since the last Firebox restart

- End date and time of CA and IPSec certificates
- CA fingerprint
- Status of the physical link (an interface or link icon in color means an interface or link is configured, and a dark icon indicates the interface or link is down)

Branch Office VPN Tunnels

Below the Firebox Status section is a section on BOVPN tunnels. There are two types of IPSec BOVPN tunnels: tunnels you create manually and tunnels you create with the Management Server.

Mobile User VPN Tunnels

When the branch office VPN tunnels are entries for Mobile User VPN tunnels, the entry shows similar information as for Branch Office VPN.

PPTP User VPN Tunnels

For PPTP User VPN tunnels, Firebox System Manager shows the user name and the quantity of sent and received packets.

Security Services

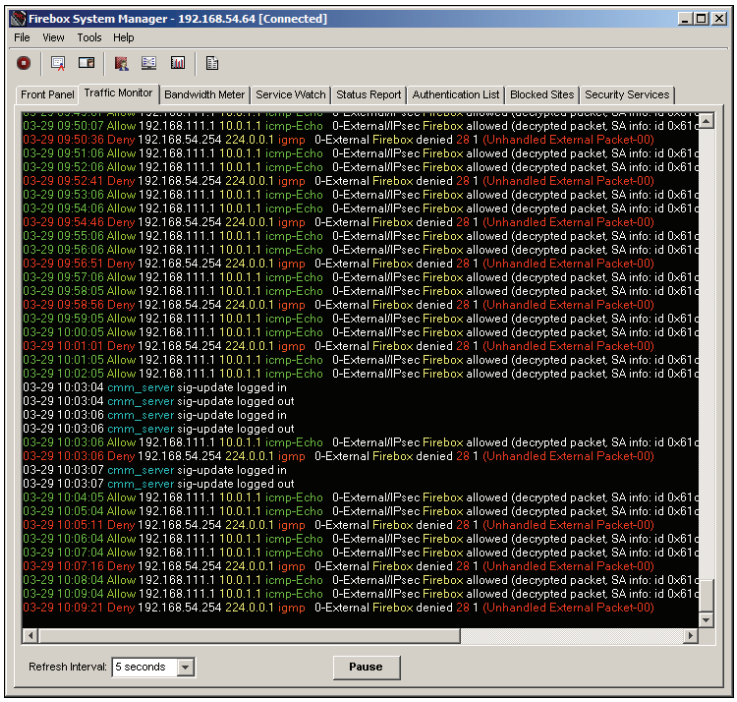
Below Security Services, Firebox System Manager includes the number of viruses found, the number of intrusions, and the number of spam e-mail messages that are blocked and effectively quarantined since the last restart.

Expanding and closing tree views

To expand a part of the display, click the plus sign (**+**) adjacent to the entry, or double-click the name of the entry. To close a part, click the minus sign (**–**) adjacent to the entry. When no plus or minus sign shows, no more information is available.

Monitoring Firebox Traffic

To see Firebox® log messages, click the **Traffic Monitor** tab.


Firebox System Manager - 192.168.54.64 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
Refresh Interval: 5 seconds
Pause

Setting the maximum number of log messages

You can change the maximum number of log messages that you can keep and see on Traffic Monitor. When you get to the maximum number, the new log messages replace the first entries. If you have a slow processor or a small quantity of RAM, a high value in this field can slow your management system. If it is necessary to examine a large volume of log messages, we recommend that you use Log Viewer, as described in "Starting LogViewer" on page 91.

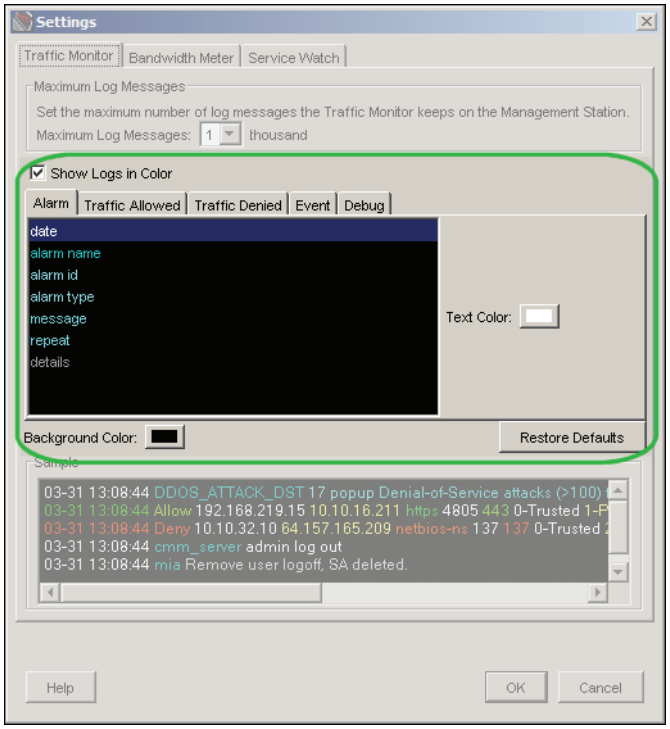
1 From Firebox System Manager, select **File > Settings**.
The Settings dialog box appears.

2 From the **Maximum Log Messages** drop-down list, select the number of log messages that you want to appear in Traffic Monitor. Click **OK**.
The value you type gives the number of log messages in thousands.

Using color for your log messages

In Traffic Monitor, you can make messages appear in different colors. Each color can refer to the types of information they show.

1 From Firebox System Manager, select **File > Settings**. Click the **Traffic Monitor** tab.



2 To disable or enable the display of colors, clear or select the **Show Logs in Color** check box.

3 On the **Alarm**, **Traffic Allowed**, **Traffic Denied**, **Event**, or **Debug** tab, click the field to appear in a color.

The Text Color field on the right side of the tabs shows the color in use for the field.

4 To change the color, click the color control adjacent to **Text Color**. Select a color. Click **OK** to close the color control dialog box. Click **OK** again to close the **Settings** dialog box.

The information in this field appears in the new color on Traffic Monitor. A sample of how Traffic Monitor looks appears at the bottom of the dialog box.

5 You can also select a background color for the traffic monitor. Click the color control arrow adjacent to **Background Color**. Select a color. Click **OK** to close the color control dialog box. Click **OK** again to close the **Settings** dialog box.

You can cancel the changes you make in this dialog box. Click **Restore Defaults**.

Copying log messages

To make a copy of a log message and paste it in a different software application, right-click the message and select **Copy Selection**. If you select **Copy All**, Firebox System Manager copies all the log messages. Open the other tool and paste the message or messages.

To copy more than one, but not all, log messages, use Log Viewer to open the log file, and then use the Log Viewer copy function, as described in the “Logging and Notification” chapter.

Learning more about a traffic log message

To learn more about a traffic log message, you can:

Copy the IP address of the source or destination

Make a copy of the source or destination IP address of a traffic log message, and paste it into a different software application. To copy the source IP address, right-click the message, and select **Source IP Address > Copy Source IP Address**. To copy the destination IP address, right-click the message, and select **Destination IP Address > Copy Destination IP Address**.

Ping the source or destination

To ping the source or destination IP address of a traffic log message, do this: Right-click the message, and select **Source IP Address > Ping** or **Destination IP Address > Ping**. A pop-up window shows the results.

Trace the route to the source or destination

To use a traceroute command to the source or destination IP address of a traffic log message, do this: Right-click the message, and select **Source IP Address** > **Trace Route** or **Destination IP Address** > **Trace Route**. A pop-up window shows you the results of the traceroute.

Temporarily block the IP address of the source or destination

To temporarily block all traffic from a source or destination IP address of a traffic log message, do this: Right-click the message, select **Source IP Address > Block: [***IP address***]** or **Destination IP Address > Block: [***IP address***]**. The length of time that an IP address is temporarily blocked by this command is set in Policy Manager. To use this command you must give the configuration password.

Clearing the ARP Cache

The ARP (Address Resolution Protocol) cache on the Firebox® keeps the hardware addresses (also known as MAC addresses) of TCP/IP hosts. Before an ARP request starts, the system makes sure that a hardware address is in the cache. You must clear the ARP cache on the Firebox after installation when your network has a drop-in configuration.

1 From Firebox System Manager, select **Tools > Clear ARP Cache**.

2 Type the Firebox configuration passphrase. Click **OK**.
This flushes the cache entries.

When a Firebox is in drop-in mode, this procedure clears only the content of the ARP table and not the MAC table. The oldest MAC entries in the MAC table are removed if the table has more than 2000 entries. If you want to clear the MAC table, you must restart the Firebox.

Using the Performance Console

The Performance Console is a Firebox® utility that you use to make graphs that show how different parts of the Firebox are operating. To get the information, you define the counters that identify the information that is used to make the graph.

Types of counters

You can monitor these types of performance counters:

System Information
Show how the CPU is used.

Interfaces
Monitor and report on the events of selected interfaces. For example, you can set up a counter that monitors the number of packets a specified interface receives.

Policies
Monitor and report on the events of selected policies. For example, you can set up a counter that monitors the number of packets that a specified policy examines.

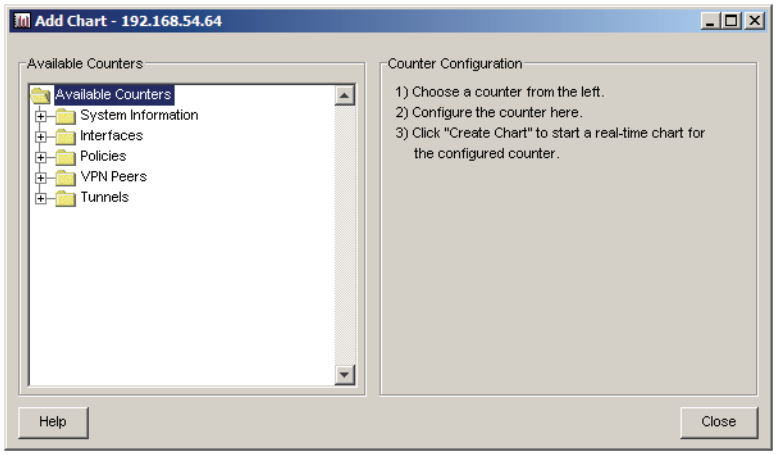
VPN Peers
Monitor and report on the events of selected VPN policies.

Tunnels
Monitor and report on the events of selected VPN tunnels.

Defining counters

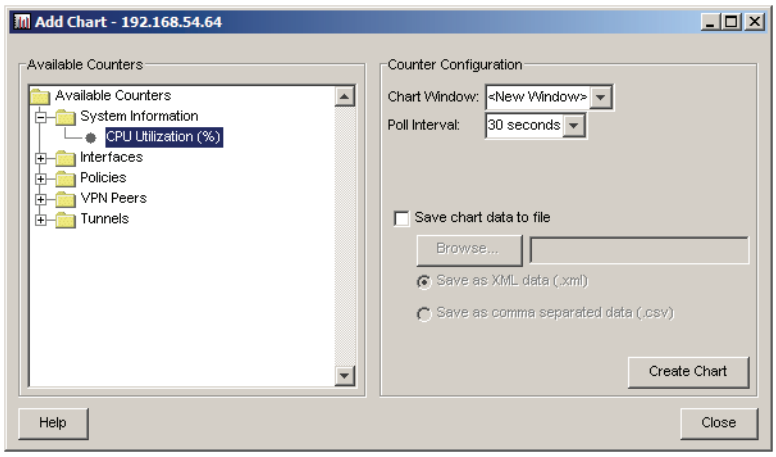
To identify a counter for any of the categories:

1 From Firebox System Manager, select the Performance Console icon. Or, select **Tools > Performance Console**.
The Add Chart window appears.



2 From the **Add Chart** window, expand one of the counter categories that appears below **Available Counters**.

Click the + sign adjacent to the category name to see the counters you can use in that category. When you click a counter, the Counter Configuration fields automatically refresh, related to the counter you select.



3 From the **Chart Window** drop-down list, select **New Window** if you want the graph to appear in a new window. Or, select the name of an open window to add the graph to a window that is open.

4 From the **Poll Interval** drop-down list, select a time interval between five seconds and one hour.

This is the frequency that the Performance Console checks for updated information from the Firebox.

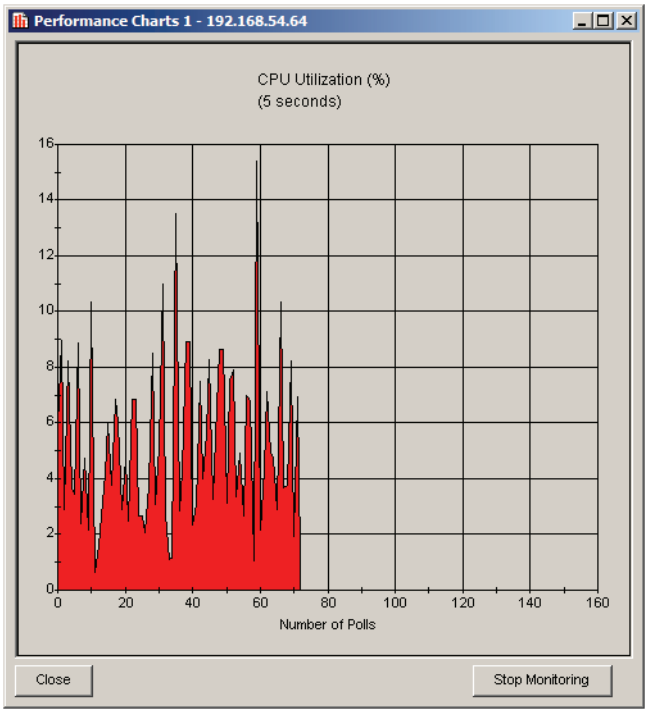
5 Add configuration information that applies to the specified counter. These fields appear automatically when you select specified counters.

- **Type** — Use the drop-down list to select the type of graph to create.
- **Interface** — Use the drop-down list to select the interface to graph data for.
- **Policy** — Use the drop-down list to select a policy from your Firebox configuration to graph data for. If you select a Policy counter, you can update the policy list that appears in the Performance Console when you click the **Refresh Policy List** button.
- **Peer IP** — Use the drop-down list to select the IP address of a VPN endpoint to graph data for. If you select a VPN Peers counter, you can update the policy list that appears in the Performance Console when you click the **Refresh Peer IP List** button.
- **Tunnel ID** — Use the drop-down list to select the name of a VPN tunnel to graph data for. If you select a Tunnels counter, you can update the policy list that appears in the Performance Console when you click the **Refresh Tunnel ID List** button. If you do not know the tunnel ID for your VPN tunnel, check the Firebox System Manager Front Panel tab.

6 Select the **Save Chart Data to File** check box to save the data collected by the Performance Console to an XML data file or a comma-separated data file.

For example, you can open an XML data file in Microsoft Excel to see the counter value recorded for each polling interval. You can use other tools to merge data from more than one chart.

7 Click **Create Chart** to start a real-time graph of this counter.



Note

This performance graph shows CPU usage. You create graphs for other functions in the same way.

Viewing the performance graph

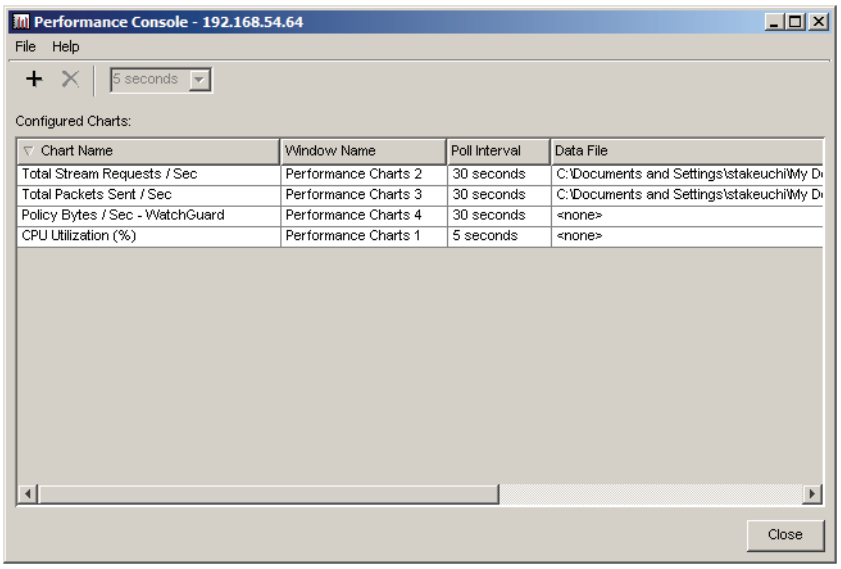
Graphs are shown in a real-time chart window. You can show one graph in each window, or show many graphs in one window. Graphs automatically scale to fit the data.

Click **Stop Monitoring** to stop the Performance Console from getting data for this counter. You can stop the monitor to save resources and restart it at different time.

Click **Close** to close the chart window.

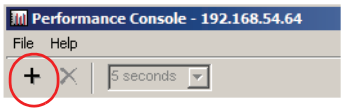
Working with more than one Performance Console graph

The main Performance Console window shows a table with all configured and active performance counters. From this window, you can add a new chart or change the polling intervals for configured counters.



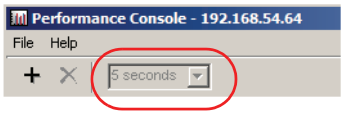
Adding a new chart

To add a new chart, click the + button on the Performance Console toolbar or select **File > Add Chart**.



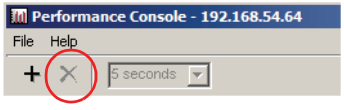
Changing the polling interval

To change the polling interval for one performance console, select the chart name from the list. Use the polling interval drop-down list on the Performance Console toolbar to change the frequency for the polls.



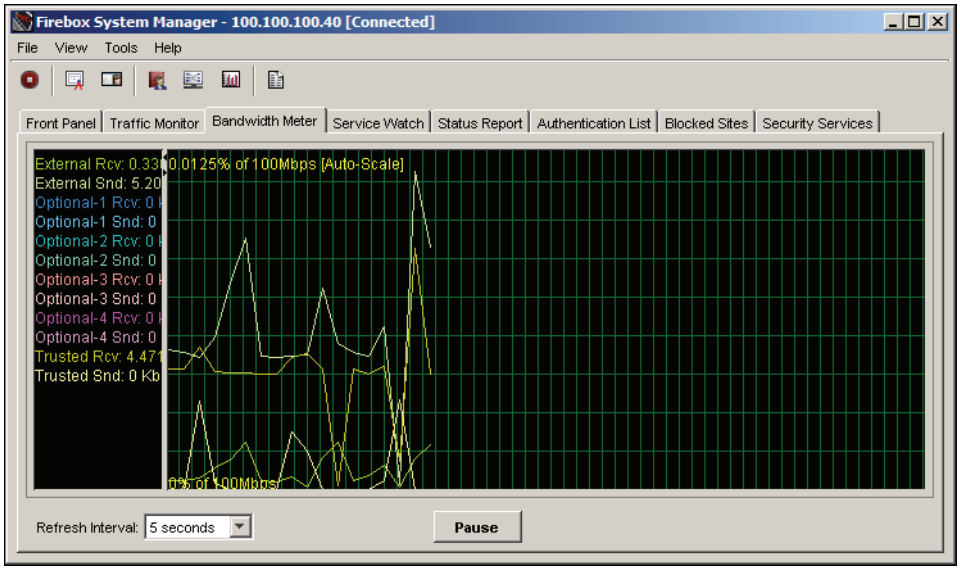
Deleting a chart

To delete a chart, select the chart name from the list and use the X button on the Performance Console toolbar or select **File > Delete Chart**.



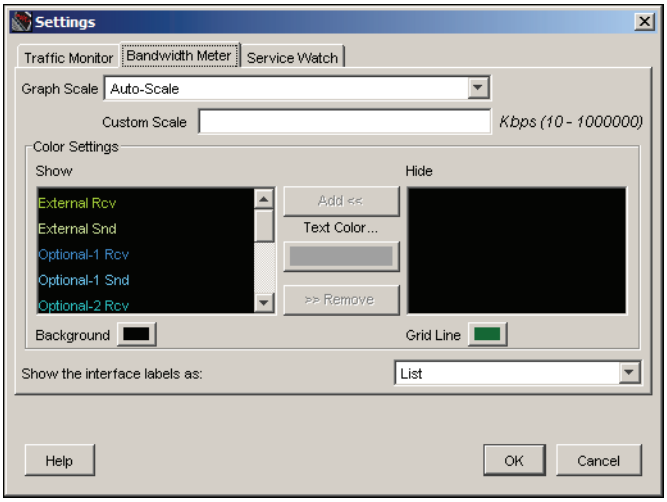
Viewing Bandwidth Usage

Select the **Bandwidth Meter** tab to see the real-time bandwidth for all the Firebox® interfaces. The Y axis (vertical) shows the number of connections. The X axis (horizontal) shows the time. If you click any location on the chart, you can get more detailed information in a pop-up window about bandwidth use at that point in time.


Firebox System Manager - 100.100.100.40 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
External Rcv: 0.33
External Snd: 5.20
Optional-1 Rcv: 0
Optional-1 Snd: 0
Optional-2 Rcv: 0
Optional-2 Snd: 0
Optional-3 Rcv: 0
Optional-3 Snd: 0
Optional-4 Rcv: 0
Optional-4 Snd: 0
Trusted Rcv: 4.47
Trusted Snd: 0 Kb
0.0125% of 100Mbps [Auto-Scale]
Refresh Interval: 5 seconds
Pause

To change how the bandwidth appears:

1 From Firebox System Manager, select **File > Settings**. Click the **Bandwidth Meter** tab.



2 Do one or more of the steps in the sections below.

Changing the scale of the bandwidth display

You can change the scale of the **Bandwidth Meter** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the speed of your network. You can also set a custom scale. Type the value in kilobytes for each second in the **Custom Scale** text box.

Adding and removing lines in the bandwidth display

- To add a line to the **Bandwidth Meter** tab, select the interface from the **Hide** list in the Color Settings section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.
- To remove a line from the **Bandwidth Meter** tab, select the interface from the **Show** list in the Color Settings section. Click **Remove**. The interface name appears in the **Hide** list.

Changing colors in the bandwidth display

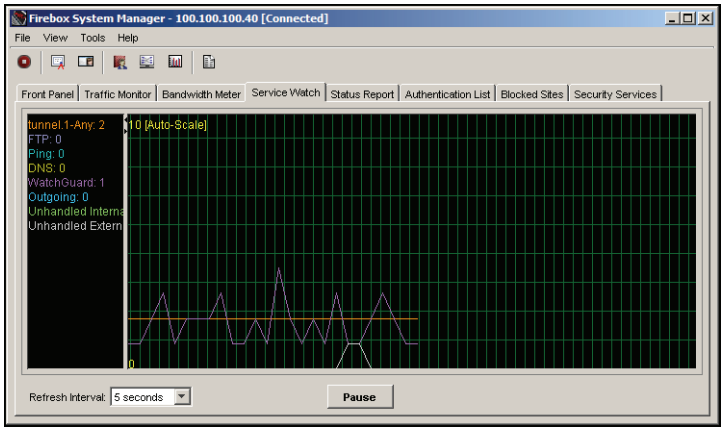
You can also change the colors of the display of the **Bandwidth Meter** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

Changing how interfaces appear in the bandwidth display

One option is to change how the interface names appear on the left side of the **Bandwidth Meter** tab. The names can appear as a list. The display can also show an interface name adjacent to the line it identifies. Use the **Show the interface** text as a drop-down list to select **List** or **Tags**.

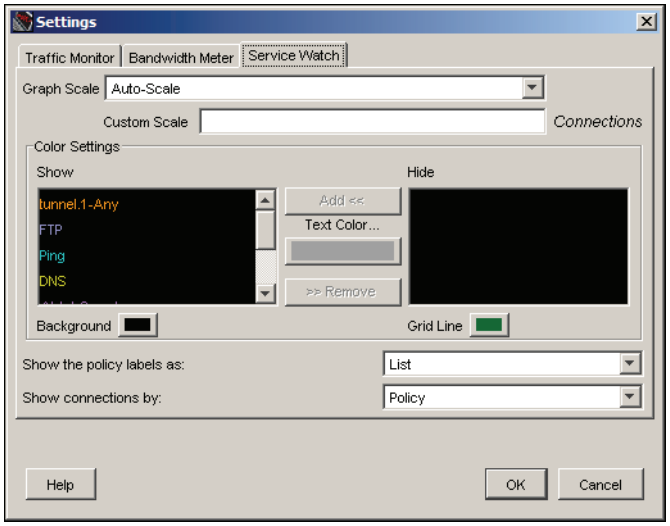
Viewing Number of Connections by Policy

Select the **Service Watch** tab of Firebox® System Manager to see a graph of the policies that are configured in Policy Manager for a Firebox. The Y axis (vertical) shows the number of connections. The X axis (horizontal) shows the time. If you click any location on the chart, you can get more detailed information in a pop-up window about policy use at this point in time.



1 To change how the policies appear, select **File > Settings**. Click the **Service Watch** tab.

2 Do one or more of the steps in the sections below.



Changing the scale of the policies display

You can change the scale of the **Service Watch** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the volume of traffic on your network. You can also set a custom scale. Type the number of connections in the **Custom Scale** text box.

Adding and removing lines in the policies display

- To add a line to the **Service Watch** tab, select the policy from the **Hide** list in the Color Settings section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.
- To remove a line from the **Service Watch** tab, select the policy from the **Show** list in the Color Settings section. Click **Remove**. The interface name appears in the **Hide** list.

Changing colors in the policies display

You can change the colors of the display of the **Service Watch** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

Changing how policy names appear in the policies display

You can change how the policy names appear on the left side of the **Service Watch** tab. The names can show as a list. The tab can also show an interface name adjacent to the line it identifies. Use the **Show the policy labels as** drop-down list to select **List** or **Tags**.

Showing connections by policy or rule

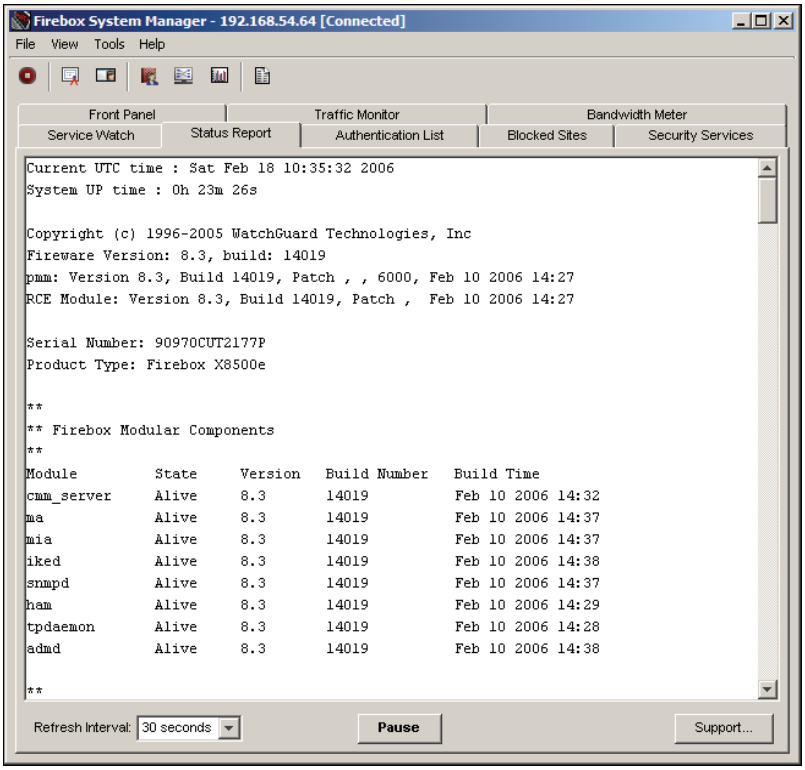
The **Service Watch** tab can show the number of connections by policy or rule. If you show by policy, then you can see more than one rule on one line. Use the **Show connections by** drop-down list to select a display setting.

Viewing Information About Firebox Status

There are four tabs that tell about Firebox® status and configuration: **Status Report**, **Authentication List**, **Blocked Sites**, and **Security Services**.

Status Report

The **Status Report** tab gives you statistics about Firebox traffic and performance.


Firebox System Manager - 192.168.54.64 [Connected]
File View Tools Help
Front Panel
Traffic Monitor
Bandwidth Meter
Service Watch
Status Report
Authentication List
Blocked Sites
Security Services
Current UTC time : Sat Feb 18 10:35:32 2006
System UP time : 0h 23m 26s
Copyright (c) 1996-2005 WatchGuard Technologies, Inc
Fireware Version: 8.3, build: 14019
pmm: Version 8.3, Build 14019, Patch , , 6000, Feb 10 2006 14:27
RCE Module: Version 8.3, Build 14019, Patch , Feb 10 2006 14:27
Serial Number: 90970CUT2177P
Product Type: Firebox X8500e
** Firebox Modular Components
Module State Version Build Number Build Time
cmm_server Alive 8.3 14019 Feb 10 2006 14:32
ma Alive 8.3 14019 Feb 10 2006 14:37
mia Alive 8.3 14019 Feb 10 2006 14:37
iked Alive 8.3 14019 Feb 10 2006 14:38
snmpd Alive 8.3 14019 Feb 10 2006 14:37
ham Alive 8.3 14019 Feb 10 2006 14:29
tpdaemon Alive 8.3 14019 Feb 10 2006 14:28
admd Alive 8.3 14019 Feb 10 2006 14:38
Refresh Interval: 30 seconds
Pause
Support...

The Firebox Status Report contains this information:

Uptime and version information
: The Firebox uptime, the WatchGuard® Firebox System software version, the Firebox model, and appliance software version. There is also a list of the status and version of the product components on the Firebox.

Log Servers
: The IP addresses of all configured Log Servers.

Logging options
: Log message options that are configured with the Quick Setup Wizard or Policy Manager.

Memory and load average
: Statistics on the memory use (shown in bytes of memory) and load average of the Firebox. The load average has three values that typically show an average over the last minute, 5 minutes, and 15 minutes. Values over 1.00 (100%) indicate some threads are queued until resources are available. (A system load that exceeds 1.00 does not mean the system is overloaded.)

Processes
The process ID, the name of the process, and the status of the process.

Network configuration
Information about the network cards in the Firebox: the interface name, its hardware and software addresses, and its netmask. The display also includes local routing information and IP aliases.

Blocked Sites list
The current manually blocked sites and any current exceptions. Temporarily blocked site entries appear on the permanent **Blocked Sites** tab.

Interfaces
Each Firebox interface appears in this section, along with information about the type of interface it is configured as (external, trusted, or optional), its status and packet count.

Routes
The Firebox kernel routing table. You use these routes to find which Firebox interface is used for each destination address.
Dynamic routes that have been accepted by the dynamic routing daemon appear here as well.

ARP table
The ARP table on the Firebox. The ARP table is used to match IP addresses to hardware addresses. (When an appliance is in drop-in mode, use the contents of the ARP table only to troubleshoot connectivity over secondary networks on the interfaces.)

Dynamic Routing
This shows dynamic routing components are in use on the Firebox, if any.

Refresh interval
This is the rate at which this display updates the information.

Support
Click **Support** to open the **Support Logs** dialog box. This is where you set the location to which you save the diagnostic log file. You save a support log in tarzipped (*.tgz) format. You create this file for troubleshooting, when asked by your support representative.

Authentication List

The **Authentication List** tab of Firebox System Manager gives information about all the persons that are authenticated to the Firebox. There are four columns to show you information about each authenticated user:

User
The name the user gives when they authenticate.

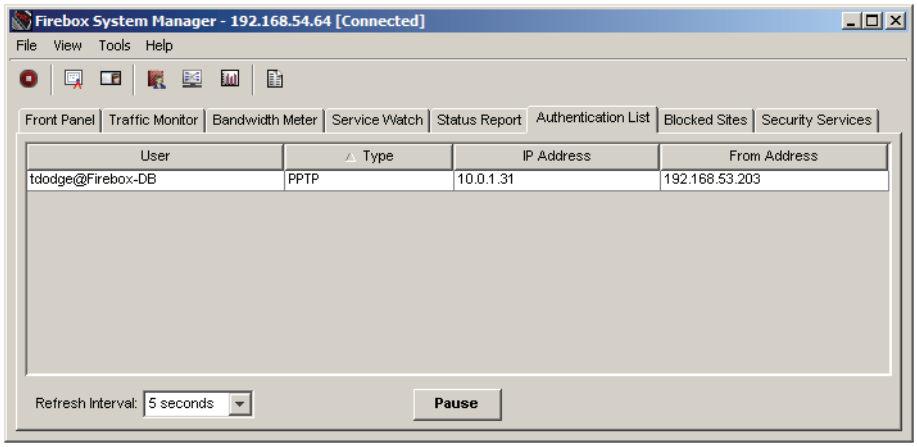
Type
The type of user who authenticated: Firewall, MUVPN, or PPTP.

IP Address
The internal IP address being used by the user. For MUVPN and PPTP users, the IP address shown here is the IP address assigned to them by the Firebox.

From Address

The IP address on the computer the user authenticates from. For MUVPN and PPTP users, the IP address shown here is the IP address on the computer they used to connect to the Firebox. For Firewall users, the IP Address and From Address are the same.

You can click the column headers to sort users. You can also remove an authenticated user from the list. To do this, right-click their user name and then stop their authenticated session.


Firebox System Manager - 192.168.54.64 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
User Type IP Address From Address
tdodge@Firebox-DB PPTP 10.0.1.31 192.168.53.203
Refresh Interval: 5 seconds
Pause

Blocked Sites

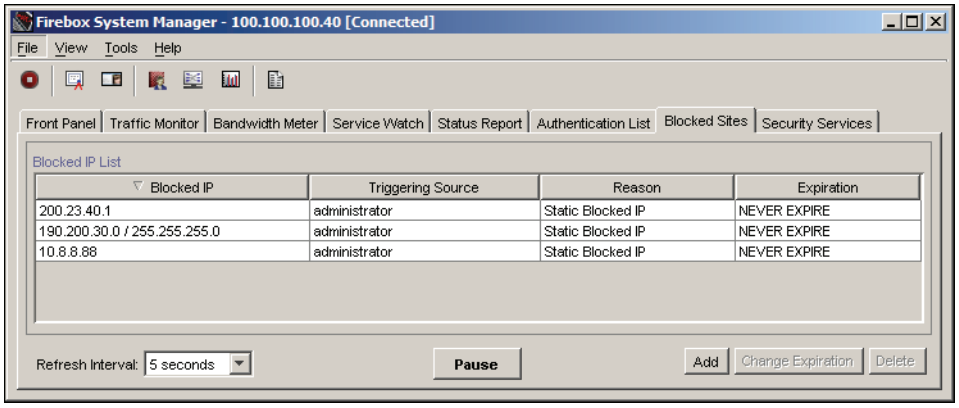
The **Blocked Sites List** tab of Firebox System Manager shows the IP addresses of all the external IP addresses that are temporarily blocked. Many events can cause the Firebox to add an IP address to the **Blocked Sites** tab: a port space probe, a spoofing attack, an address space probe, or an event you configure.

Adjacent to each IP address is the time when it comes off the **Blocked Sites** tab. You can use the **Blocked Sites** dialog box in Policy Manager to adjust the length of time that an IP address stays on the list.

Adding and removing sites

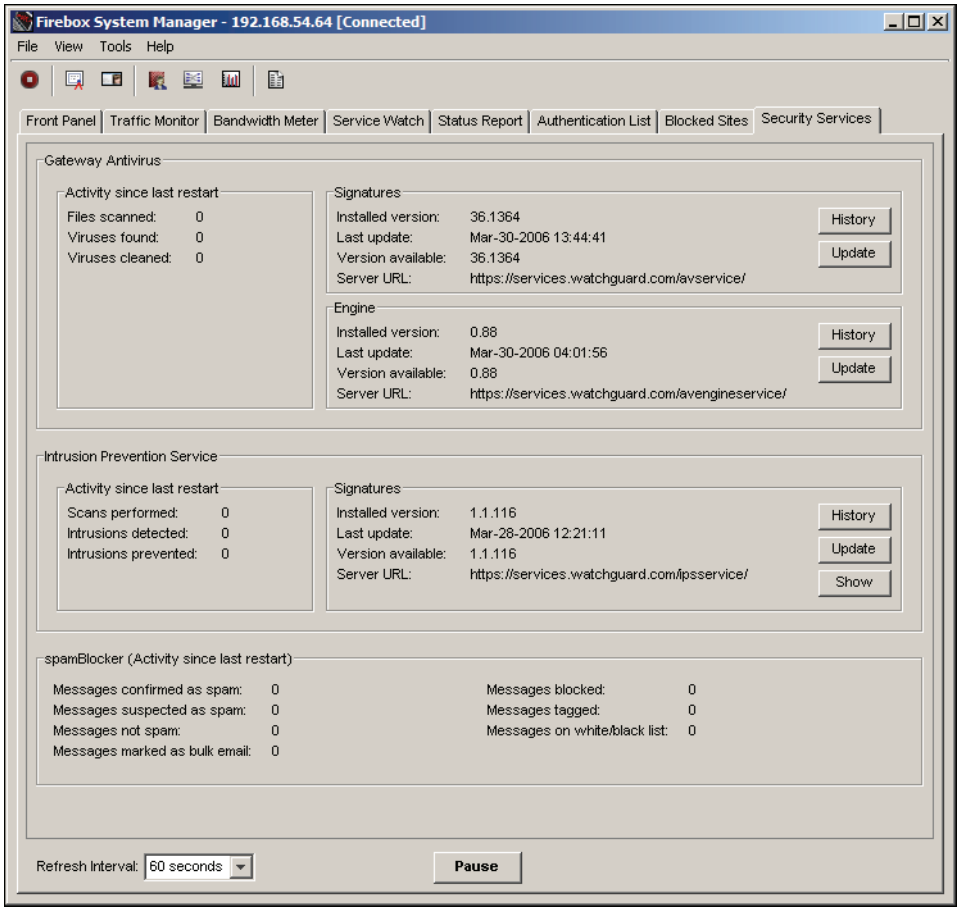
Add allows you to temporarily add a site to the blocked sites list. Click **Change Expiration** to change the time at which this site is deleted from the list. **Delete** removes the site from the blocked sites list.

You can remove a site from the list only if you open the Firebox with the configuration passphrase.


Firebox System Manager - 100.100.100.40 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
Blocked IP List
Blocked IP
Triggering Source
Reason
Expiration
200.23.40.1 administrator Static Blocked IP NEVER EXPIRE
190.200.30.0 / 255.255.255.0 administrator Static Blocked IP NEVER EXPIRE
10.8.8.88 administrator Static Blocked IP NEVER EXPIRE
Refresh Interval: 5 seconds
Pause
Add
Change Expiration
Delete

Security Services

The **Security Services** tab includes information about the Gateway AntiVirus and Intrusion Prevention services.



Gateway AntiVirus

This area of the dialog box gives information about the Gateway AntiVirus feature.

Activity since last restart

- Files scanned: Number of files scanned for viruses since the last Firebox restart.
- Viruses found: Number of viruses found in scanned files since the last Firebox restart.
- Viruses cleaned: Number of infected files deleted since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates.
- Update: Click to update your virus signatures. This button is active only if a new version of the virus signatures is available.

Engine

- Installed version: Version number of the installed engine.
- Last update: Date of the last engine update.
- Version available: If a new version of the engine is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the engine updates.
- Update: Click to update your antivirus engine. This button is active only if a new version of the engine is available.

Intrusion Prevention Service

This area of the dialog box gives information about the Signature-Based Intrusion Prevention Service feature.

Activity since last restart

- Scans performed: Number of files scanned for viruses since the last Firebox restart.
- Intrusions detected: Number of viruses found in scanned files since the last Firebox restart.
- Intrusions prevented: Number of infected files deleted since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates.
- Update: Click this button to update your intrusion prevention signatures. This button is active only if a new version of the intrusion prevention signatures is available.

- Show: Click this button to download and show a list of all current IPS signatures. After you download the signatures, you can look for signatures by signature ID.

spamBlocker

Activity since last restart

- Number of messages that are identified as not spam, spam, bulk, or suspect e-mail.
- Number of messages that are blocked and tagged.
- Number of messages that are blocked or allowed because of a spamBlocker exceptions list that you create (exceptions that you create to deny additional sites are sometimes known as a blacklist; exceptions that you create to allow additional sites are sometimes known as a whitelist).

Using HostWatch

HostWatch is a graphic user interface that shows the network connections between the trusted and external networks. HostWatch also gives information about users, connections, and network address translation (NAT).

The line that connects the source host and the destination host uses a color that shows the type of connection. You can change these colors. The default colors are:

- **Red** — The Firebox® denies the connection.
- **Blue** — The connection uses a proxy.
- **Green** — The Firebox uses NAT for the connection.
- **Black —** Normal connection (the connection has been accepted, and it does not use a proxy or NAT).

Icons that show the type of service appear adjacent to the server entries for HTTP, Telnet, SMTP, and FTP.

Domain name server (DNS) resolution does not occur immediately when you start HostWatch. When HostWatch is configured for DNS resolution, it replaces the IP addresses with the host or user names. If the Firebox cannot identify the host or user name, the IP address stays in the HostWatch window.

If you use DNS resolution with HostWatch, the management station can send a large number of NetBIOS packets (UDP 137) through the Firebox. The only method to stop this is to turn off NetBIOS over TCP/IP in Windows.

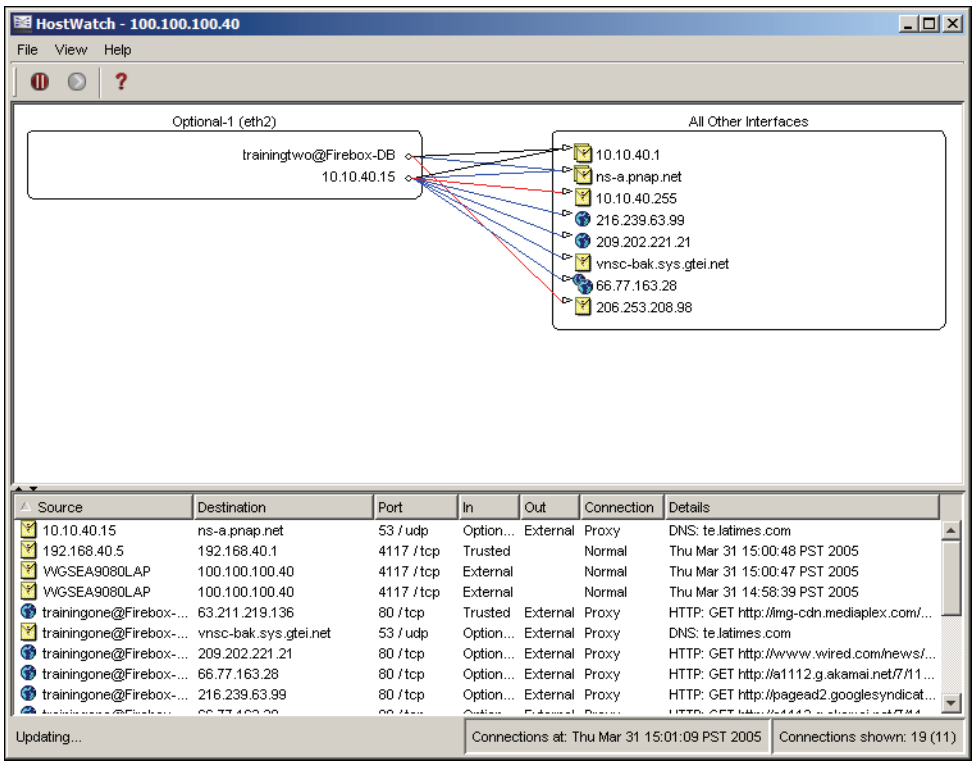
To start **HostWatch**, click the **HostWatch** icon in Firebox System Manager.
Or select **Tools > HostWatch**.

The HostWatch window

The top part of the HostWatch window has two sides. You can set the interface for the left side. The right side shows all other interfaces. HostWatch shows the connections to and from the interface configured on the left side. To select an interface, right-click the current interface name. Select the new interface.

Double-click an item on one of the sides to get the **Connections For** dialog box for connections that involve that item. The dialog box shows information about the connection, and includes the IP addresses, port number, time, connection type, and direction.

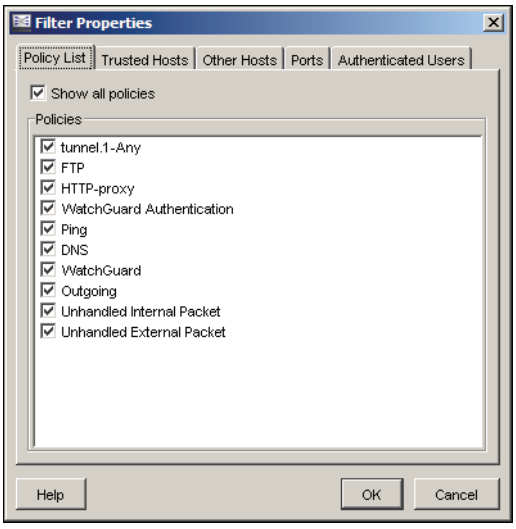
While the top part of the window only shows the connections to and from the selected interface, the bottom of the HostWatch window shows all connections to and from all interfaces. The information is shown in a table with the ports and the time the connection was created.


HostWatch - 100.100.100.40
File View Help
Optional-1 (eth2)
trainingtwo@Firebox-DB
10.10.40.15
All Other Interfaces
10.10.40.1
ns-a.pnap.net
10.10.40.255
216.239.63.99
209.202.221.21
vnsc-bak.sys.gtei.net
66.77.163.28
206.253.208.98
Source Destination Port In Out Connection Details
10.10.40.15 ns-a.pnap.net 53 / udp Option... External Proxy DNS: te.latimes.com
192.168.40.5 192.168.40.1 4117 / tcp Trusted Normal Thu Mar 31 15:00:48 PST 2005
WGSEA9080LAP 100.100.100.40 4117 / tcp External Normal Thu Mar 31 15:00:47 PST 2005
WGSEA9080LAP 100.100.100.40 4117 / tcp External Normal Thu Mar 31 14:58:39 PST 2005
trainingone@Firebox-... 63.211.219.136 80 / tcp Trusted External Proxy HTTP: GET http://img-cdn.mediaplex.com/...
trainingone@Firebox-... vnsc-bak.sys.gtei.net 53 / udp Option... External Proxy DNS: te.latimes.com
trainingone@Firebox-... 209.202.221.21 80 / tcp Option... External Proxy HTTP: GET http://www.wired.com/news/...
trainingone@Firebox-... 66.77.163.28 80 / tcp Option... External Proxy HTTP: GET http://a1112.g.akamai.net/7/11...
trainingone@Firebox-... 216.239.63.99 80 / tcp Option... External Proxy HTTP: GET http://pagead2.googlesyndicat...
Updating...
Connections at: Thu Mar 31 15:01:09 PST 2005
Connections shown: 19 (11)

Controlling the HostWatch window

You can change the HostWatch window to show only the necessary items. You can use this feature to monitor specified hosts, ports, or users.

1 From HostWatch, select **View > Filter**.



2 Click the tab to monitor: **Policy List**, **External Hosts**, **Other Hosts**, **Ports**, or **Authenticated Users**.

3 On the tab for each item you do not want to see, clear the check boxes in the dialog box.

4 On the tab for each item you do want to see, type the IP address, port number, or user name to monitor. Click **Add**. Do this for each item that HostWatch must monitor.

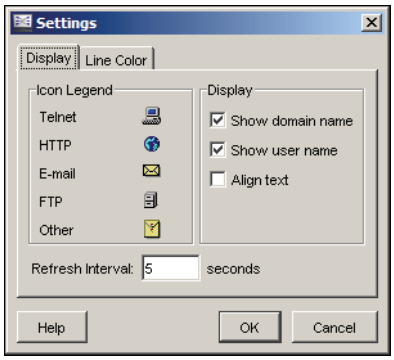
5 Click **OK**.

Changing HostWatch view properties

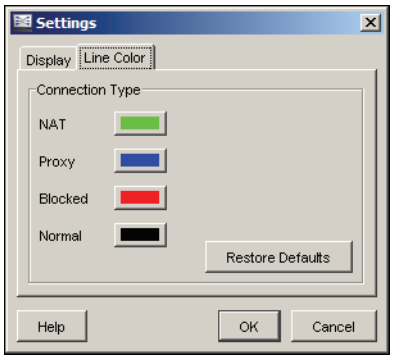
You can change how HostWatch shows information. For example, HostWatch can show host names as an alternative to addresses.

1 From HostWatch, select **View > Settings**.

2 Use the **Display** tab to change how the hosts appear in the HostWatch window.



3 Use the **Line Color** tab to change the colors of the lines between NAT, proxy, blocked, and normal connections.



4 Click **OK** to close the **Settings** dialog box.

Adding a blocked site from HostWatch

To add an IP address to the blocked sites list from HostWatch, right-click on the connection and use the pop-up window to select the IP address from the connection to add to the blocked sites list. You must set the time for the IP address to be blocked, and give the configuration passphrase.

Pausing the HostWatch display

You can use the **Pause** and **Continue** icons on the toolbar to temporarily stop and then restart the display. Or, use **File > Pause** and **File > Continue**.

CHAPTER 5

Basic Firebox Administration

To operate correctly, your Firebox® must have the necessary information to apply your security policy to the traffic that goes through your network. Policy Manager gives you one user interface to configure basic Firebox settings in addition to your security policy. This chapter shows you how to:

- Add, delete, and view licenses
- Set up the Firebox to use an NTP server
- Set the Firebox time zone
- Configure the Firebox for SNMP
- Change the Firebox passphrases
- Give the Firebox a name for easy identification (instead of an IP address)
- Recover a Firebox

Working with Licenses

You increase the functionality of your Firebox® when you purchase an option and add the license key to the configuration file. When you get a new key, make sure that you use the instructions that come with the key to activate the new feature on the LiveSecurity web site and add a new feature key to your Firebox.

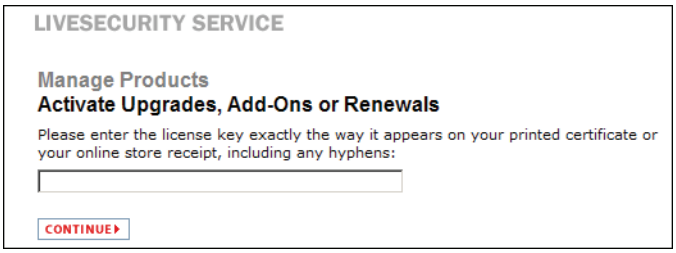
Activating a new feature

Before you activate a new feature, you must have a license key certificate from WatchGuard® that is not already registered on the LiveSecurity web site. This license key comes on a paper license key certificate, or on your online store receipt (if you purchased from the WatchGuard online store).

1 Open a web browser and connect to https://www.watchguard.com/activate.

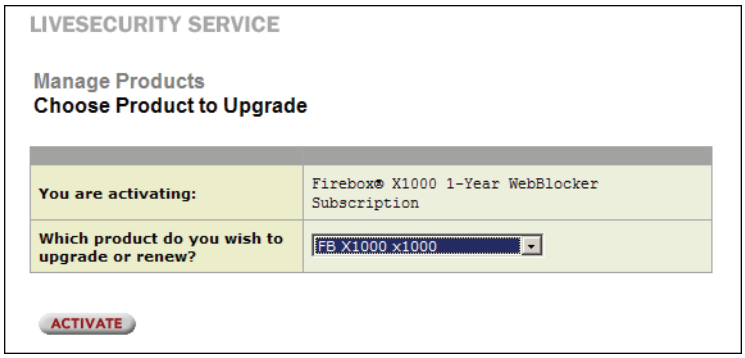
2 If you have not already logged in to LiveSecurity, you are directed to the LiveSecurity Log In page. Type your LiveSecurity user name and passphrase.

3 Below **Options**, select **Upgrades, Renewals, Services**. Click **Continue**.
The Activate Upgrades, Add-Ons, or Renewals page appears.


LIVESECURITY SERVICE
Manage Products
Activate Upgrades, Add-Ons or Renewals
Please enter the license key exactly the way it appears on your printed certificate or your online store receipt, including any hyphens:
CONTINUE

4 Type the license key for the product as it appears on your printed certificate, including the hyphens.

5 Click **Continue**.
The Choose Product to Upgrade page appears.

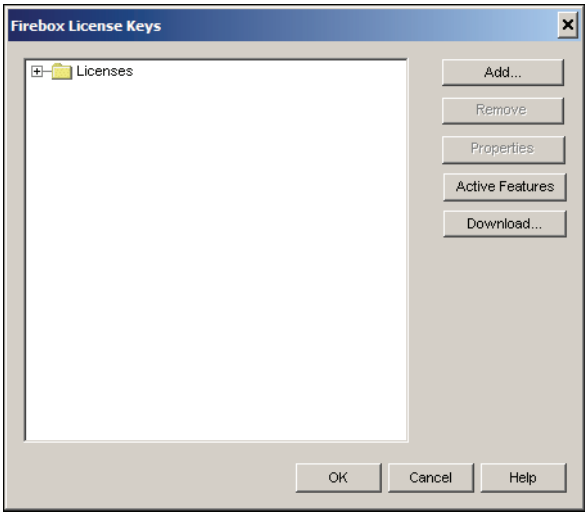


6 From the drop-down list, select the Firebox to which you want to apply the upgrade or renewal. If you added a Firebox name when you registered your Firebox, that name appears in this list. After you select the Firebox, click **Activate**.

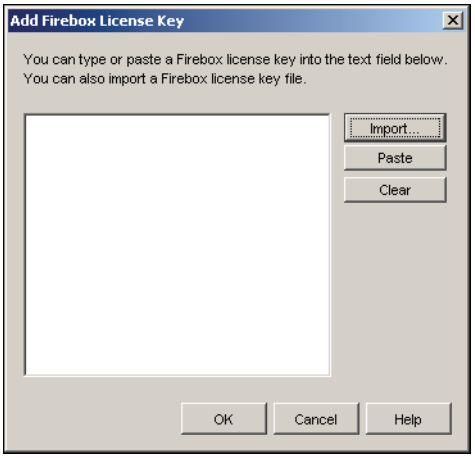
7 The Retrieve Feature Key page appears. From your Windows Start menu, open Notepad or any application into which you can save text. Copy the full feature key from this page to a text file and save it on your computer. Click **Finish**.

Adding licenses

1 From Policy Manager, select **Setup > Licensed Features**.
The Firebox License Keys dialog box appears. This dialog box shows the licenses that are available.



2 Click **Add**.
The Add Firebox License Key dialog box appears. We recommend that you remove the old feature key before you add a new feature key.



3 Click **Import** and find the feature key file or paste the contents of your feature key file into the dialog box.

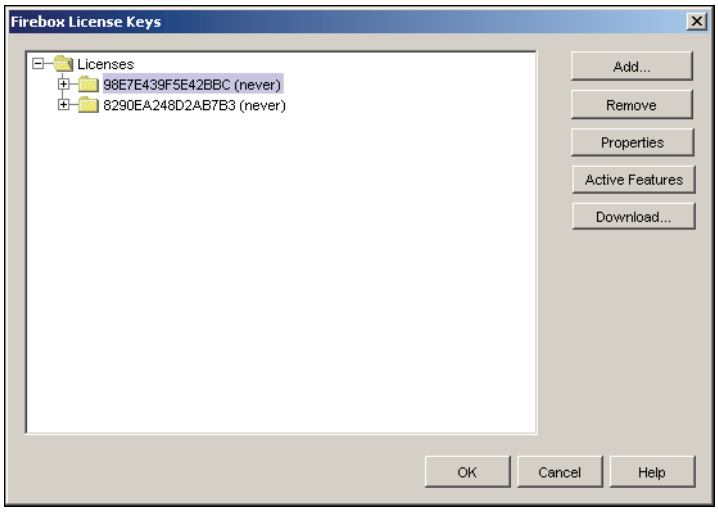
4 Click **OK** two times.
At this time, the features are available on the management station. In some conditions, new dialog boxes and menu commands to configure the feature appear in Policy Manager.

5 Save the configuration to the Firebox.
The feature does not operate on the Firebox until you save the configuration file to the Firebox.

Deleting a license

1 From Policy Manager, select **Setup > Licensed Features**.
The Firebox License Keys dialog box appears.

2 Expand **Licenses**, select the license ID you want to delete, and click **Remove**.

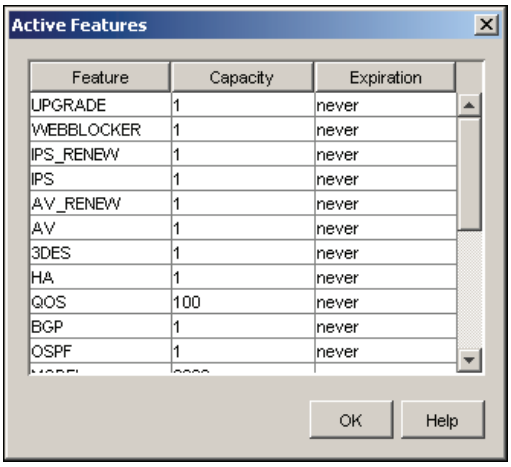


3 Click **OK**.

4 Save the configuration to the Firebox.

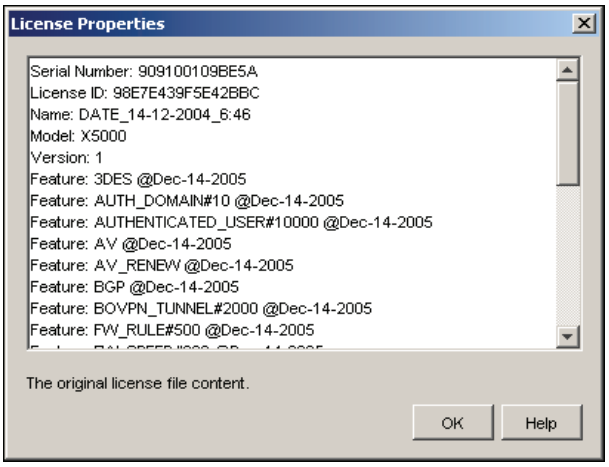
Seeing the active features

To see a list of all features with licenses, select the license key and click **Active Features**. The **Active Features** dialog box shows each feature along with its capacity and expiration.



Seeing the properties of a license

To see the properties of a license, select the license key and click **Properties**. The **License Properties** dialog box shows the serial number of the Firebox to which this license applies, along with its ID and name, the Firebox model and version number, and the available Firebox features.



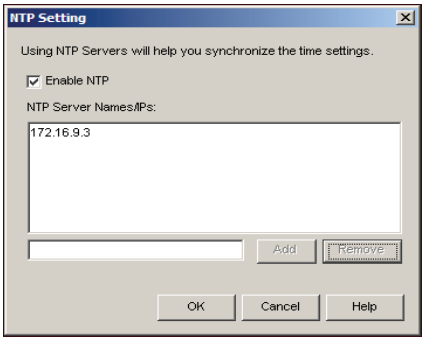
Downloading a license key

If your license file is not current, you can download a copy of any license file from the Firebox to your management station. To download license keys from a Firebox, select the license key and click **Download**. A dialog box appears for you to type the status passphrase of the Firebox.

Setting NTP Servers

Network Time Protocol (NTP) synchronizes computer clock times across a network. The Firebox® can synchronize its clock to an Internet NTP server.

1 From Policy Manager, select **Setup > NTP**.
The NTP Setting dialog box appears.



2 Select the **Enable NTP** check box.

3 In the box below the **NTP Server Names/IPs** list, type the IP addresses of the NTP servers you want to use. Click **Add**.
The Firebox can use up to three NTP servers.

4 Click **OK**.

Setting a Friendly Name and Time Zone

You can give the Firebox® a special name to use in your log files and reports. If you do not do this procedure, the log files and reports use the IP address of the Firebox external interface. Many customers use a Fully Qualified Domain Name if they register such a name with the DNS system. You must give the Firebox a special name if you use the Management Server to configure VPN tunnels and certificates with the Firebox.

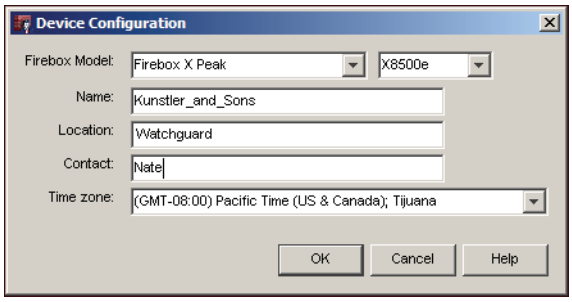
The Firebox time zone controls the date and time that appear in the log file and on tools such as LogViewer, Historical Reports, and WebBlocker. Set the Firebox time zone to the time zone for the physical location of the Firebox. This time zone setting allows for the time to appear correctly in the log messages. The Firebox system time is set to Greenwich Mean Time (GMT) by default.

1 From Policy Manager, click **Setup > System**.
The Device Configuration dialog box appears.

2 In the **Name** text box, type the special name you want for the Firebox. Click **OK**.
A pop-up notification tells you if you use characters that are not allowed.

3 In the **Location** and **Contact** fields, type any information that could be helpful ito identify and maintain the Firebox.

4 From the **Time zone** drop-down list, select the time zone you want. Click **OK**.



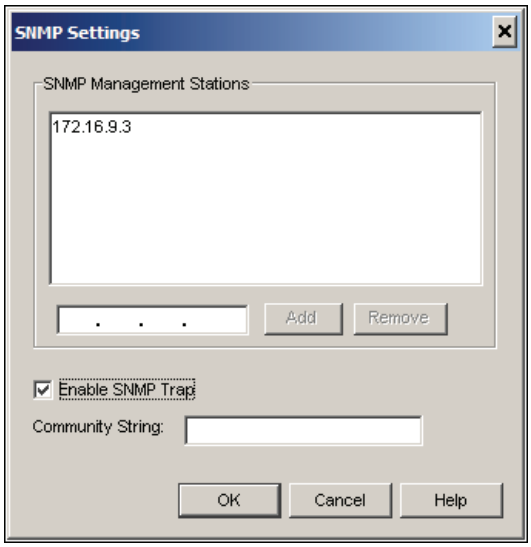
Working with SNMP

Simple Network Management Protocol (SNMP) is a set of tools for monitoring and managing networks. SNMP uses management information bases (MIBs) that give configuration information for the devices the SNMP server manages or monitors. With Fireware® appliance software, the Firebox® supports SNMPv1 and SNMPv2c.

You can configure the Firebox to accept SNMP polls from an SNMP server. You can also configure the Firebox to send traps to an SNMP server.

Enabling SNMP polling

1 From Policy Manager, select **Setup > SNMP**.



2 Type the **Community String** the Firebox must use when it connects to the SNMP server. Click **OK**.
The community string allows access to the statistics of a device. It operates like a wireless SSID or group ID. This community string must be included with all SNMP requests. If the community string is correct, the device gives the requested information. If the community string is not correct, the device discards the request and does not respond.

3 Click **OK**. Save the configuration to the Firebox.
The Firebox can now receive SNMP polls.

Enabling SNMP traps

An SNMP trap is an event notification the Firebox sends to the SNMP management system. The trap identifies when a condition occurs, such as a value that is more than its predefined threshold.

To enable the Firebox to send SNMP traps:

1 From Policy Manager, select **Setup > SNMP.**

2 In the **SNMP Settings** dialog box, select the **Enable SNMP Trap** check box.

3 In the box below the **SNMP Management Stations** list, type the IP address of the SNMP server. Click **Add**.

4 Type the **Community String** the Firebox must use when it connects to the SNMP server. Click **OK**.
The community string is like a user ID or password that allows access to the statistics of a device. This community string must be included with all SNMP requests. If the community string is correct, the device gives the requested information. If the community string is not correct, the device discards the request and does not respond.

5 Add an SNMP policy to the Firebox. To do this, from Policy Manager, select **Edit > Add Policy** (or click the "+" icon), expand **Packet Filters**, select **SNMP**, and click **Add**.
The New Policy Properties dialog box appears.

6 Below the **From** box, click **Add**. From the **Add Address** dialog box that appears, click **Add Other**.
The Add Member dialog box appears.

7 From the **Choose Type** drop-down list select **Host IP**. In the **Value** field, type the IP address of your SNMP server computer.

8 Click **OK** twice to return to the **Policy** tab of the new policy.

9 Below the **To** box, click **Add**.

10 From the **Add Address** dialog box that appears, under **Available Members**, select **Firebox**. Click **Add**.

11 Click **OK**, **OK**, and **Close**. Save the configuration to the Firebox.

You can make the Firebox send a trap for any policy in Policy Manager. Edit the policy that will trigger a trap. To do this, double-click the policy icon shown in Policy Manager to edit the configuration. From the **Edit Policy Properties** dialog box, select the **Properties** tab. Click **Logging** and select the **Send SNMP Trap** check box.

Using MIBs

WatchGuard® System Manager with Fireware® appliance software supports two types of Management Information Bases (MIBs):

- Public MIBs are used in the Fireware product and are copied on to your WatchGuard management station when you install Fireware. These MIBs include IETF standards and MIB2.
- Private MIBs are MIBs created by WatchGuard to provide basic monitoring information for specific components in the Firebox, including CPU and memory utilization, and interface and IPSec metrics.

When you install WatchGuard System Manager, MIBs are installed to My Documents\My WatchGuard\Shared WatchGuard\SNMP.

The Firebox supports these read-only object MIBs:

- RFC1155-SMI
- SNMPv2-SMI
- RFC1213-MIB
- RAPID-MIB
- RAPID-SYSTEM-CONFIG-MIB

Changing the Firebox Passphrases

A Firebox® uses two passphrases:

- Status passphrase
  The read-only password or passphrase that allows access to the Firebox
- Configuration passphrase
  The read-write passwordor passphrase that allows an administrator full access to the Firebox

To create a secure passphrase, we recommend that you:

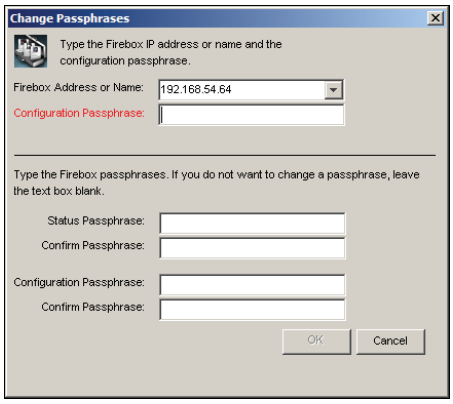
- Use a selection of uppercase and lowercase characters, numbers, and special characters (for example, Im4e@tiN9).
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language. Make a new acronym that only you know.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.

An additional security measure is to change the Firebox passphrases at regular intervals. To do this, you must have the configuration passphrase.

1 From Policy Manager, open the configuration file on the Firebox.

2 Click **File > Change Passphrases**.
An Open Firebox dialog box appears.

3 From the **Firebox** drop-down list, select a Firebox or type the IP address or name of the Firebox. Type the Firebox configuration (read/write) passphrase. Click **OK**.
The Change Passphrases dialog box appears.


Change Passphrases
Type the Firebox IP address or name and the configuration passphrase.
Firebox Address or Name:
192.168.54.64
Configuration Passphrase:
Type the Firebox passphrases. If you do not want to change a passphrase, leave the text box blank.
Status Passphrase:
Confirm Passphrase:
Configuration Passphrase:
Confirm Passphrase:
OK
Cancel

4 Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase.

5 Click **OK**.
The new flash image and the new passphrases save to the Firebox. The Firebox automatically starts again.

Recovering a Firebox

If you want to reset a Firebox® to its factory-default settings or reset a Firebox with a completely new configuration, you can use a Firebox recovery procedure. The procedure to recover a Firebox X Core or Peak e-Series device is different from the procedure to recover an earlier model of a Firebox X Core or Peak. Make sure you use the correct procedure for your Firebox.

Resetting a Firebox X e-Series device

To put a new configuration on a Firebox X Core or Peak e-Series device, use the Web Quick Setup Wizard. See the "Getting Started" chapter for more information on the Web Quick Setup Wizard.

Resetting a Firebox X Core or Peak (non e-Series)

When you reset an earlier model Firebox X Core or Peak, you replace the existing image on the Firebox with a new image. You can use the Quick Setup Wizard to reset a Firebox with a completely new configuration. This is the easiest way to reset a Firebox and the most common procedure used.

There are times, however, when you cannot use the Quick Setup Wizard to reset a Firebox. When you use the Quick Setup Wizard, you must be able to make a network connection to the Firebox from your management station and "discover" the Firebox on the network. If this is not possible, you can use the manual reset procedure described in this manual.

You must have a current Firebox feature key before you begin this procedure.

To manually reset the Firebox:

1 Turn the Firebox off. On the front of the Firebox, find and press the up arrow.

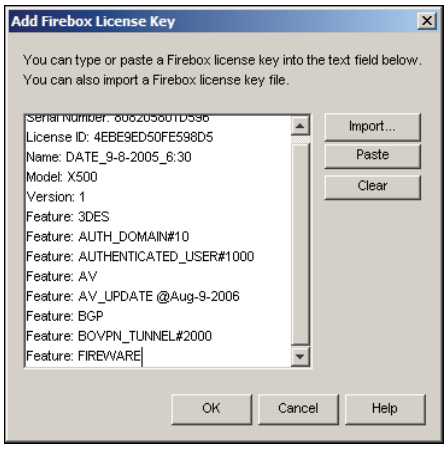
2 Hold down the up arrow button while you turn on the Firebox, and continue to hold the button down until the LCD display shows the Firebox is running in System B or Safe mode.
When the Firebox is running in System B mode, it is running in factory-default mode. In factory-default mode, the Firebox trusted interface is set to 10.0.1.1.

3 Connect a cross-over Ethernet network cable between your WatchGuard management station and the trusted interface of the Firebox.
The trusted interface is labeled interface 1 on the Firebox.

4 Change the IP address on your management station to 10.0.1.2 (or another IP address from which you can connect to the Firebox trusted interface at 10.0.1.1).
It is a good idea to ping the trusted interface from your management station to make sure you have an operational network connection.

5 Open Policy Manager. You can open an existing configuration file, or create a new configuration file using the options available from the **File** drop-down menu.

6 Select **Setup > Licenses Features**. Click **Add** and paste a copy of your feature key in the text box, if necessary.



7 When you are ready, select **File > Save > To Firebox**. Save your configuration to the Firebox at IP address 10.0.1.1, with the administrative passphrase "admin".

8 After the Firebox restarts with its new configuration, it is a good idea to change the passphrases for the Firebox. Select **File > Change Passphrases** to set new passphrases.

9 You can now put the Firebox back on to your network and connect to it using the IP addresses and passphrases you set in your new configuration.
If you did not change the IP address or passphrase, you can connect to the trusted IP address 10.0.1.1 with the passphrase "admin".

Resetting a Firebox using fbxinstall

If the Quick Setup Wizard and the manual reset procedure do not correct the problem, you can reset the Firebox to its factory-default settings with the command line utility, fbxinstall. This procedure puts a

new filesystem and operating system on the Firebox flash disk and is necessary if your flash disk is corrupted. Before you start, make sure you have Fireware® installed on your management station.

To use fbxinstall:

1 Connect a serial cable between the Firebox and your management station.
If you have more than one COM port, note which port you use.

2 Connect the trusted interface of the Firebox to the Ethernet port on your management station with a cross-over cable.

3 Change the IP address on your management station to 10.10.10.2/24. Set the default gateway on your management station to 10.10.10.1.

4 Open a command prompt.

5 Type `fbxinstall 10.10.10.2/24`
This IP address is used to connect to the Firebox to complete the reset process, but is not actually assigned to the Firebox.

6 When the fbxinstall process is complete, start the Quick Setup Wizard to set a new configuration to your Firebox.
Remember to reset your management station IP address and default gateway back to their original state when you are done with the fbxinstall procedure.

CHAPTER 6

Basic Configuration Setup

After your Firebox® is installed on your network and operates with a basic configuration file, you can start to add custom configuration settings to align with your organization requirements. This chapter shows you how to do some basic configuration and maintenance tasks. Some of these tasks you complete many times as you work with your Firebox. Other tasks you do only one time.

These basic configuration tasks include:

- Open a configuration file on a local computer or from the Firebox
- Save a configuration file to a local computer or the Firebox
- Create and restore a Firebox backup image
- Use aliases
- Configure Firebox global settings
- Set basic schedules to use in your policies later
- Manage your Firebox from a remote location

Opening a Configuration File

Policy Manager for Fireware® or Fireware Pro is a software tool that lets you make, change, and save configuration files. A configuration file, with the extension.xml, includes all configuration data, options, IP addresses, and other information that makes up your Firebox® security policy. When you use Policy Manager, you see a version of your configuration file that is easy to examine and change.

When you work with Policy Manager, you can:

- Open the current configuration file on your Firebox
- Open a configuration file saved on your local hard drive
- Make a new configuration file

Opening a working configuration file

A common task for a network administrator is to make a change to your current security policy. For example, your business purchases a new software application, and you must open a port and protocol

to a server at a vendor location. For this task, you must change your configuration file with Policy Manager.

Using WatchGuard System Manager

1 From the Windows desktop, click **Start > All Programs > WatchGuard System Manager 8.3 > WatchGuard System Manager**.
WatchGuard® System Manager 8.3 is the default name of the folder for the Start menu icons. You can change this folder name during installation.

2 From WatchGuard System Manager, select **File > Connect To Device**.

Or,
click the Connect to Device icon on the WatchGuard System Manager toolbar. The Connect to Firebox dialog box appears.

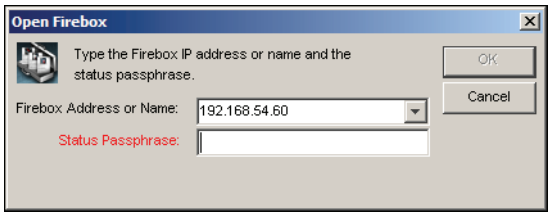
3 Use the drop-down list to select your Firebox, or type its trusted IP address. Type the status passphrase. Click **OK**.
The device appears in the WatchGuard System Manager Device Status tab.

4 Select the Firebox on the **Device Status** tab. Then, select **Tools > Policy Manager**.

Or,
click the Policy Manager icon on the WatchGuard System Manager toolbar. Policy Manager opens, and it puts the configuration file in use on the selected Firebox.

Using Policy Manager

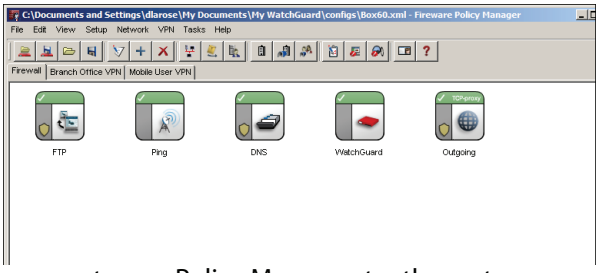
1 From Policy Manager, click **File > Open > Firebox**.
The Open Firebox dialog box appears.
If you get an error message that tells you that you cannot connect, try again.



2 From the **Firebox Address or Name** drop-down list, select a Firebox.
You can also type the IP address or host name.

3 In the **Passphrase** text box, type the Firebox status (read-only) passphrase.
Use the status passphrase here. You must use the configuration passphrase to save a new configuration to the Firebox.

4 Click **OK**.
Policy Manager opens the configuration file and shows the settings.



If you cannot open Policy Manager, try these steps:

- If the **Connect to Firebox** dialog box immediately comes back after you enter the passphrase, make sure that Caps Lock is off and that you type the passphrase correctly. Remember that the passphrase is case-sensitive.

- If the **Connect to Firebox** dialog box times out, make sure that you have a link on the trusted interface and on your computer. Make sure that you typed the correct IP address for the trusted interface of the Firebox. Also make sure that your computer IP address is in the same network as the trusted interface of the Firebox.

Opening a local configuration file

Some network administrators find it helps to save more than one version of a Firebox configuration file. For example, if you have a new security policy to use, we recommend that you save the old configuration file to a local hard drive first. Then if you do not want the new configuration, you can restore the old version. You can open configuration files that are on any network drive to which your management station can connect.

1 From WatchGuard System Manager, select **Tools > Policy Manager** (or click the Policy Manager icon).

2 Select **File > Open > Configuration File**.

Or,
click the Open File icon on the Policy Manager toolbar. A standard Windows open file dialog box appears.

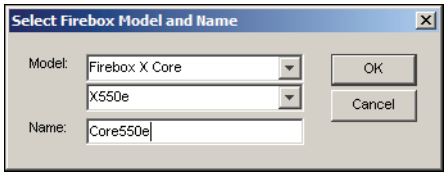
3 Use the **Open** dialog box to find and to select the configuration file. Click **Open**.
Policy Manager opens the configuration file and shows the settings.

Making a new configuration file

The Quick Setup Wizard makes a basic configuration file for your Firebox. We recommend that you use this as the base for each of your configuration files. However, you can also use Policy Manager to make a new configuration file with only the default configuration properties.

1 From WatchGuard System Manager, select **Tools > Policy Manager** (or click the Policy Manager icon).

2 From Policy Manager, select **File > New**.
The Select Firebox Model and Name dialog box appears.



3 Use the **Model** drop-down lists to select your Firebox model. Because there are groups of features that are unique to each model, select the same model as your hardware device.

4 Type a name for the Firebox to appear as the name of the configuration file.

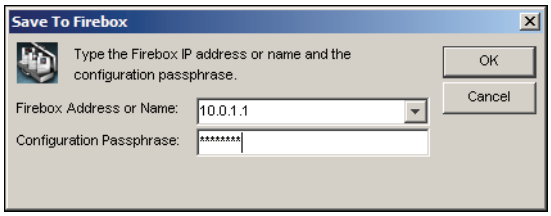
5 Click **OK**.
Policy Manager makes a new configuration with the file name <name>.xml, where <name> is the name you gave the Firebox.

Saving a Configuration File

After you make a new configuration file or change the current configuration file, you can save it directly to the Firebox®. You can also save it to a local hard disk.

Saving a configuration to the Firebox

1 From Policy Manager, click **File > Save > To Firebox**.
The Save to Firebox dialog box appears.



2 From the **Firebox Address or Name** drop-down list, type an IP address or name, or select a Firebox. If you use a Firebox name, the name must resolve through DNS.
When you type an IP address, type all the numbers and the periods. Do not use the TAB key or arrow key.

3 Type the Firebox configuration passphrase. You must use the configuration passphrase to save a file to the Firebox.

4 Click **OK**.

Saving a configuration to a local hard drive

1 From Policy Manager, click **File > Save > As File**.
You can also use CTRL-S. A standard Windows save file dialog box appears.

2 Type the name of the file.
The default procedure is to save the file to the WatchGuard® directory. You can also browse to any folder to which you can connect from the management station. For better security, we recommend that you save the files in a safe folder with no access to other users.

3 Click **Save**.
The configuration file saves to the local hard drive.

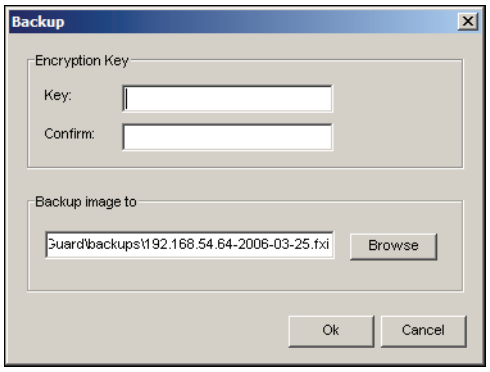
About Firebox Backup Images

A Firebox backup image is an encrypted and saved copy of the flash disk image from the Firebox flash disk. It includes the Firebox appliance software, configuration file, licenses and certificates. You can save a backup image to your management station or to a directory on your network. We recommend that you regularly make backup files of the Firebox image. We also recommend that you create a backup image of the Firebox before you make significant changes to your Firebox configuration or upgrade your Firebox or its appliance software.

Creating a Firebox backup image

1 From Policy Manager, select **File > Backup**.

2 Type the configuration passphrase for your Firebox.
The Backup dialog box appears.



3 Type and confirm an encryption key.
This key is used to encrypt the backup file. If you lose or forget this encryption key, you will not be able to restore the backup file.

4 Select the directory in which to save the backup file. Click **OK**.
The default location for a backup file with a ".fxi" extension is C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address> - <date>.fxi.

Restoring a Firebox backup image

1 From Policy Manager, select **File > Restore**.

2 Type the configuration passphrase for your Firebox. Click **OK**.

3 Type the encryption key you used when you created the backup image.
The Firebox restores the backup image and restarts. It uses the backup image on restart. Wait for two minutes before you connect to the Firebox again.

If you cannot successfully restore your Firebox image, you can reset the Firebox with the procedure shown in "Recovering a Firebox" on page 65.

Working with Aliases

An alias is a shortcut that identifies a group of hosts, networks, or interfaces. When you use an alias, it is easy to create a security policy because the Firebox® allows you to use aliases when you create policies.

These are some default aliases included in Policy Manager that you can use:

Any-Trusted
This is an alias for all Firebox interfaces configured as "trusted" interfaces (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

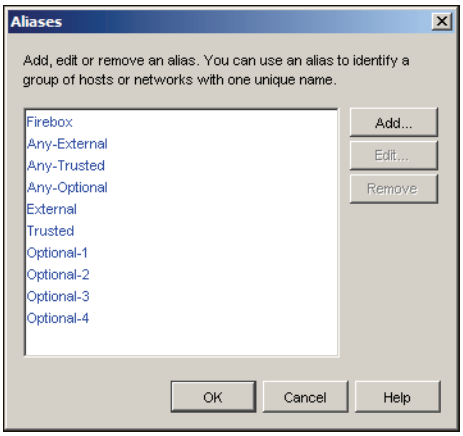
Any-External
This is an alias for all Firebox interfaces of type "external" (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

Any-Optional
These are aliases for all Firebox interfaces of type "optional" (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

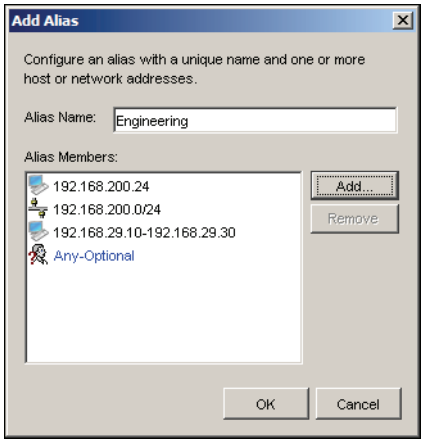
Alias names are different from user or group names used in user authentication. With user authentication, you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet protocols. For more information about user authentication, see “How User Authentication Works” on page 111.

Creating an alias

1 From Policy Manager, select **Setup > Aliases**.
The Aliases dialog box appears.



2 Click **Add**.
The Add Alias dialog box appears.



3 In the **Alias Name** text box, type a unique name to identify the alias.
This name appears in lists when you configure a security policy.

4 Click **Add** to add a host IP address, a network IP address, a host range, or an alias to the list of alias members.
The member appears in the list of alias members.

5 Click **OK** two times.

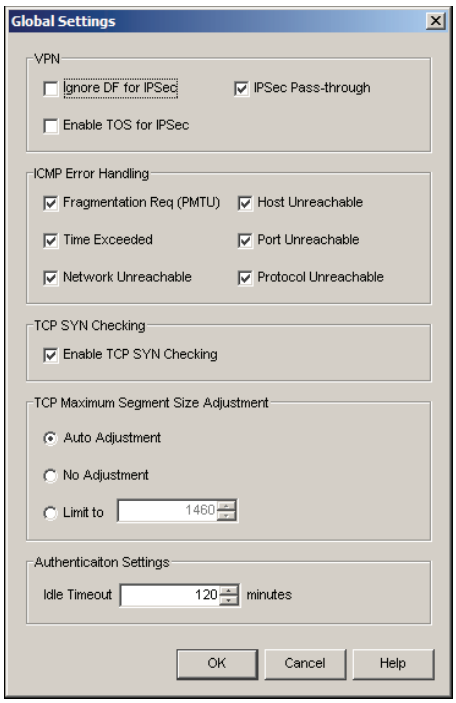
Using Global Settings

In Policy Manager you can select settings that control the actions of many Firebox® features. You set basic parameters for:

- IPSec VPN
- ICMP error handling
- TCP SYN checking
- TCP maximum size adjustment
- Authentication idle time-out

1 From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.

2 Configure the different categories of global settings as shown in the sections below.



VPN

The global VPN settings are:

Ignore DF for IPSec

Ignore the setting of the **Don't Fragment** bit in the IP header. If you set this to ignore, the Firebox breaks the frame into pieces that can fit in an IPSec packet with the ESP or AH header.

IPSec pass through

If a user must make IPSec connections to a Firebox from behind a different Firebox, you must keep the **IPSec Pass-through** check box clear to enable the IPSec pass-through feature. For example, if mobile employees are at a customer location that has a Firebox, they can make IPSec connections to their network using IPSec. For the local Firebox to correctly allow the outgoing IPSec connection, you must also add an IPSec policy to Policy Manager.

Enable TOS for IPSec

The Type of Service (TOS) bits are a set of four-bit flags in the IP header that can tell routing devices to give an IP datagram more or less priority than other datagrams. Fireware® gives you the option to allow IPSec tunnels to pass T0S flagged packets. Some ISPs drop all packets that have TOS flags set.

If you do not select the **Enable TOS for IPSec** check box, all IPSec packets have no TOS bits set. If the TOS bits were set before, when Fireware encapsulates the packet in an IPSec header, the TOS bits are cleared.

When the **Enable TOS for IPSec** check box is selected, if the original packet has TOS bits set then Fireware keeps the TOS bits set when it encapsulates the packet in an IPSec header. If the original packet does not have the TOS bits set, Fireware does not set the TOS bits when it encapsulates the packet in an IPSec header.

ICMP error handling

Internet Control Message Protocol (ICMP) controls errors during connections. It is used for two types of operations:

- To tell client hosts about error conditions.
- To probe a network to find general characteristics about the network.

The Firebox sends an ICMP error message each time an event occurs that matches one of the parameters you selected. If you deny these ICMP messages, you can increase security by preventing network probes, but it can also cause time-out delays for incomplete connections and can cause application problems. The global ICMP error handling parameters and their descriptions are:

Fragmentation Req (PMTU)

The IP datagram must be fragmented, but this is prevented because the Don't Fragment bit in the IP header is set.

Time Exceeded

The datagram was dropped because the Time to Live field expired.

Network Unreachable

The datagram could not get to the network.

Host Unreachable

The datagram could not get to the host.

Port Unreachable

The datagram could not get to the port.

Protocol Unreachable

The protocol piece of the datagram cannot be delivered.

TCP SYN checking

The global TCP SYN checking setting is:

Enable TCP SYN checking

This feature makes sure that the TCP three-way handshake is done before the Firebox allows a data connection.

TCP maximum segment size adjustment

The TCP segment can be set to a specified size for a connection that must have more TCP/IP layer 3 overhead (like PPPoE, ESP, AH, and so on). If this size is not correctly configured, users cannot get access to some web sites. The global TCP maximum segment size adjustment settings are:

Auto Adjustment
The Firebox examines all maximum segment size (MSS) negotiations and changes the MSS value to the applicable one.

No Adjustment
The Firebox does not change the MSS.

Limit to
You set a size adjustment limit.

Authentication settings

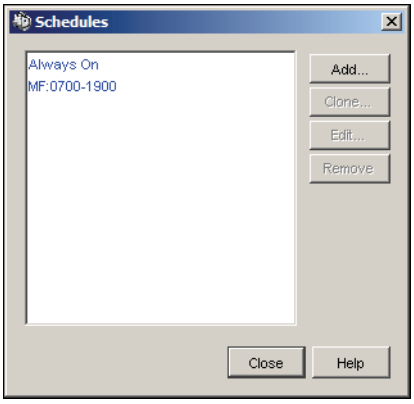
The global authentication setting is:

Idle Timeout
Set the authentication idle time-out in minutes. An authenticated user session stops automatically if the user does not make a connection that uses authentication before the time-out occurs.

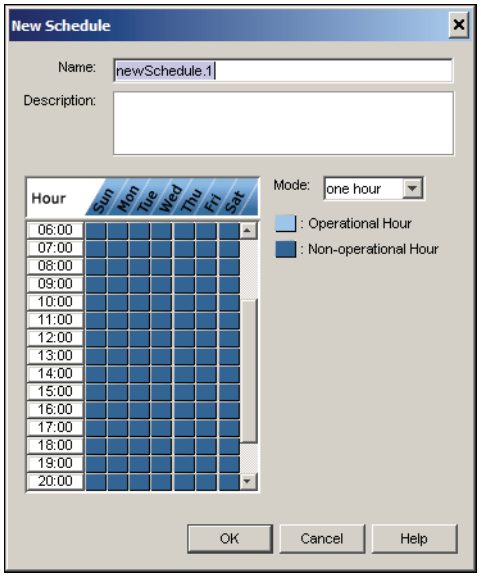
Creating Schedules

You can use schedules to automate some Firebox® actions such as WebBlocker tasks. You can create a schedule for all days of the week, or create a different schedule for each day of the week. You can then use these schedules in policies that you create. For information on how to use schedules in policies, see the "Configuring Policies" chapter.

1 From Policy Manager, select **Setup > Actions > Schedules**.
The Schedules dialog box appears.



2 Click **Add**.
The New Schedule dialog box appears.



3 Type a schedule name and description. The schedule name appears in the **Schedule** dialog box. Make sure that the name is easy to remember.

4 From the **Mode** drop-down list, select the time increment for the schedule: one hour, 30 minutes, or 15 minutes.
The chart on the left of the New Schedule dialog box shows your entry in the drop-down list.

5 The chart in the dialog box shows days of the week along the x-axis (horizontal) and increments of the day on the y-axis (vertical). Click boxes in the chart to change them between operational hours (when the policy is active) and non-operational hours (when the policy is not in effect).

6 Click **OK** to close the **New Schedule** dialog box. Click **Close** to close the **Schedules** dialog box.

To edit a schedule, select the schedule name in the **Schedule** dialog box and click **Edit**.
To create a new schedule from an existing one, select the schedule name and click **Clone**.

Managing a Firebox from a Remote Location

When you configure a Firebox® with the Quick Setup Wizard, a policy is created automatically that allows you to connect to and administer the Firebox from any computer on the trusted or optional networks. If you want to manage the Firebox from a remote location (any location external to the Firebox), then you must change your configuration to allow administrative connections from your remote location.

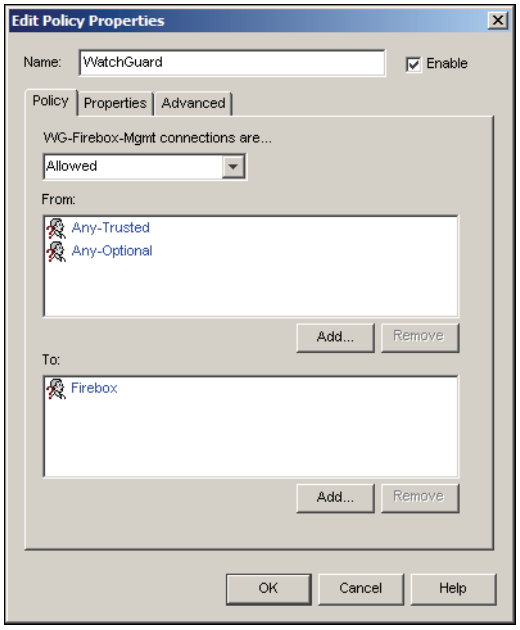
The policy that controls administrative connections to the Firebox itself is called the WatchGuard® policy in Policy Manager. This policy controls access to the Firebox on these four TCP ports: 4103, 4105, 4117, 4118. When you allow connections in the WatchGuard policy, you allow connections to each of these four ports.

Before you change a policy to allow connections to the Firebox from a computer external to your network, it is a good idea to consider:

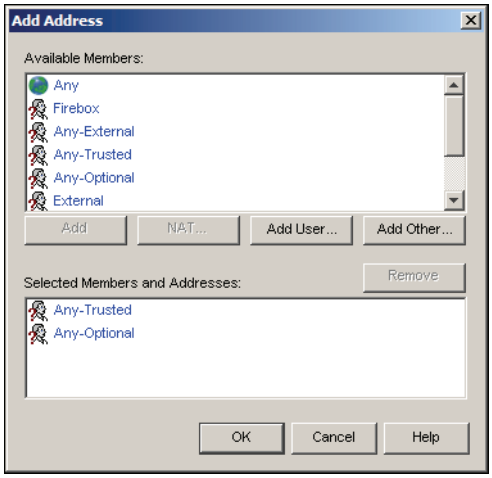
- The use of user authentication to restrict connections to the Firebox.

- It is a good idea to restrict access from the external network to the smallest number of computers possible. For example, it is more secure to allow connections from a single computer than it is to allow connections from the alias "Any-External".

1 From Policy Manager, double-click on the **WatchGuard** policy.
You can also right-click the WatchGuard policy and select Edit. The Edit Policy Properties dialog box appears.



2 Below the **From** list, click **Add**.



3 To enter the IP address of the external computer that connects to the Firebox, click **Add Other**. Make sure **Host IP** is the selected type, and type the IP address.
To add a user name, click **Add User**. Select the type of user and the method of authentication they use. From the **User/Group** drop-down list, select **User** and type the name of the user who will connect to the Firebox.

4 Click **OK**.

CHAPTER 7

Logging and Notification

An event is one activity that occurs at the Firebox®. For example, denying a packet from going through the Firebox is an event. Logging is the recording of these events to a log host. A notification is a message sent to the administrator by the Firebox when an event occurs that is a possible security threat. Notification can be an e-mail or a pop-up window, or sent by way of an SMTP trap.

For example, WatchGuard® recommends that you configure default packet handling to send a notification when the Firebox finds a port space probe. When this occurs, the log host sends notification to the network security administrator about the rejected packets. The network security administrator can examine the log files and make decisions about how to add more security to the organization's network. Some possible changes are:

- Block the ports on which the probe was used
- Block the IP address that is sending the packets
- Tell the ISP through which the packets are being sent

Logging and notification are important to a good network security policy. Together, they make it possible to monitor your network security, identify attacks and attackers, and address security threats and challenges.

You can install the Log Server on the computer you are using as a management station. Or, you can install the Log Server software on a different computer using the WatchGuard System Manager installation program and selecting to install only the Log Server component. You can also add additional Log Servers for backup.

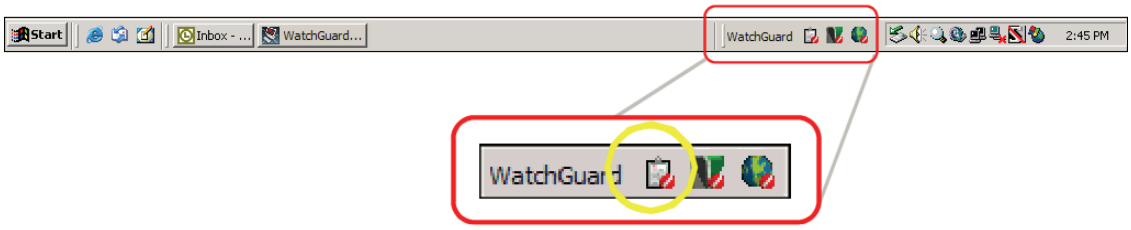
Note

If you install the Management Server, Log Server, or WebBlocker Server on a computer with a firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See "Installing WatchGuard Servers on computers with desktop firewalls" on page 20 for more information.

Setting Up the Log Server

The Log Server collects logs from each WatchGuard® Firebox® managed by WSM.

1 On the computer that has the Log Server software installed, select the Log Server icon from the WatchGuard toolbar.
If the WatchGuard toolbar does not appear, right-click in the system tray and select Toolbars > WatchGuard.,



The **WatchGuard Log Server Configuration** dialog box appears.

WatchGuard Log Server Configuration
Welcome to the...
Log Server Configuration Wizard
The first thing you must do is enter the log encryption key. This key will be used to encrypt all logs that are sent over the network.
Log Encryption Key:
Retype Log Encryption Key:
Second, please select a logging and reporting directory. This directory will store all your log, report and report definition files.
C:\Documents and Settings\WatchGuard
...
OK
Cancel
WatchGuard

2 Type the encryption key to use for the secure connection between the Firebox and the Log Servers. Log Server encryption keys are a minimum of eight characters.

3 Confirm the encryption key.

4 Select a directory to keep all logs, reports, and report definition files. We recommend that you use default location.

5 Click **OK**.

6 Click **Start > Control Panel**. Go to Power Options. Select the **Hibernate** tab and disable hibernation. This is to prevent the Log Server from shutting down when the computer hibernates.

7 Make sure the Log Server and the Firebox are set to the same system time. For information on setting system time, see the "Basic Firebox Administration" chapter.

Changing the Log Server encryption key

To change the encryption key on the Log Server:

1 Right-click the Log Server icon on the WatchGuard toolbar and select **Status/Configuration**.

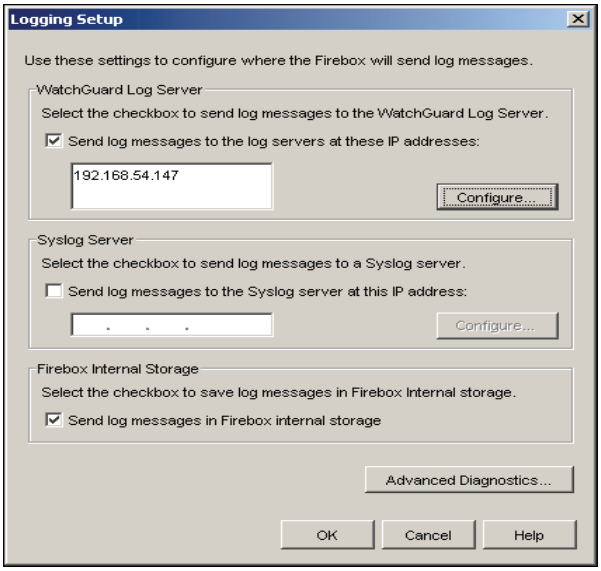
2 Select **File > Set Log Encryption Key**.

3 Type the new log encryption key two times.
4 In Policy Manager, select **Logging** and type the new log encryption key.
5 Click **OK**.
6 Do the same procedure on the Firebox.

Setting up the Firebox for a Designated Log Server

It is recommended that you have a minimum of one Log Server to use WatchGuard System Manager. You can select a different primary Log Server and one or more backup Log Servers.

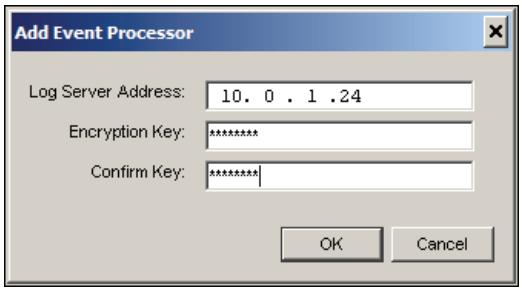
1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2 Select the Log Server or servers you want to use. Click the **Send log messages to the Log Servers at these IP addresses** check box.


Logging Setup
Use these settings to configure where the Firebox will send log messages.
WatchGuard Log Server
Select the checkbox to send log messages to the WatchGuard Log Server.
Send log messages to the log servers at these IP addresses:
192.168.54.147
Configure...
Syslog Server
Select the checkbox to send log messages to a Syslog server.
Send log messages to the Syslog server at this IP address:
Configure...
Firebox Internal Storage
Select the checkbox to save log messages in Firebox internal storage.
Send log messages in Firebox internal storage
Advanced Diagnostics...
OK
Cancel
Help

Adding a Log Server for a Firebox

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Click **Configure**. Click **Add**.
The Add Event Processor dialog box appears.



3 In the **Log Server Address** box, type the IP address of the Log Server you want to use.

4 In the **Encryption Key** and **Confirm** boxes, type the Log Server encryption key. The allowed range for the encryption key is 8–32 characters. You can use all characters but spaces and slashes (/ or \).

5 Click **OK**. Click **OK** to close the **Configure Log Servers** dialog box. Click **OK** to close the **Logging Setup** dialog box.

6 Save the changes to the Firebox to begin logging.

You can verify that the Firebox is logging correctly. From WSM, select **Tools > Firebox System Manager**. In the **Detail** section on the left, next to **Log Server**, you should see the IP address of the log host.

Setting Log Server priority

If the Firebox cannot connect to the Log Server with the highest priority, it connects to the subsequent Log Server in the priority list. If the Firebox examines each Log Server in the list and cannot connect, it tries to connect to the first Log Server in the list again. You can create a priority list for Log Servers.

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Click **Configure**.
The Configure Log Servers dialog box appears.

3 Select a Log Server from the list in the **Configure Log Servers** dialog box. Use the **Up** and **Down** buttons to change the order.

Activating syslog logging

Syslog is a log interface developed for UNIX but also used by a number of computer systems. You can configure the Firebox to send log information to a syslog server. A Firebox can send log messages to a Log Server and a syslog server at the same time, or send log messages to one or the other. Syslog log messages are not encrypted. We recommend that you do not select a host on the external interface.

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Select the **Send Log Messages to the Syslog server at this IP address** check box.

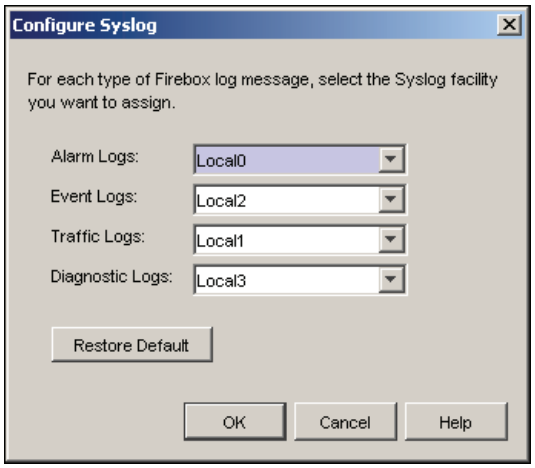
3 In the address box, type the IP address of the syslog server.

4 Click **Configure**.
The Configure Syslog dialog box appears.

5 For each type of log message, select the syslog facility to which you want it assigned. For information on types of log messages, see "Types of Log Messages" on page 90.

The syslog facility refers to one of the fields in the syslog packet and to the file the syslog is sent to. You can use Local0 for high priority syslog messages, such as alarms. You can use Local1- Local 7 to assign priorities for other types of log messages (with lower numbers having greater priority). See your syslog documentation for more information on logging facilities.

6 Click **OK**. Click **OK** to close the **Logging Setup** dialog box.



7 Save your changes to the Firebox.

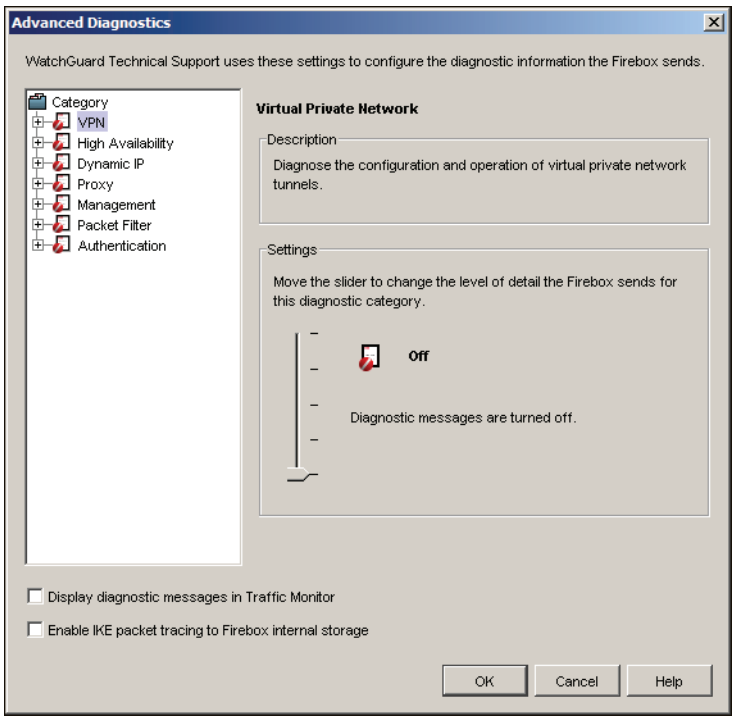
Enabling advanced diagnostics

You can select the level of diagnostic logging to write to your log file or to Traffic Monitor. We do not recommend that you set the logging level to the highest level unless a technical support representative tells you to in order to troubleshoot a problem. It can cause the log file to fill up very quickly. It can also make an high load on the Firebox.

1 From Policy Manager, select **Setup > Logging**.

The Logging Setup dialog box appears.

2 Click **Advanced Diagnostics**.
The Advanced Diagnostics dialog box appears.



3 Select a category from the category list.
A description of the category appears in the Description box.

4 Use the slider below **Settings** to set the level of information that a log of each category includes in its log message. When the lowest level is set, diagnostic messages for that category are turned off. When the highest level is set, you can set the detail level for the diagnostic log messages.

5 To show diagnostic messages in Traffic Manager, select the **Display diagnostic messages in Traffic Monitor** check box. This can be useful to quickly diagnose a problem.

6 To have the Firebox collect a packet trace for IKE packets, select the **Enable IKE packet tracing to Firebox internal storage** check box. To see the packet trace information the Firebox collects, start Firebox System Manager and click the **Status** tab. Click **Support** to have Firebox System Manager get the packet trace information from the Firebox.

7 Remember to turn off diagnostic logs when done.

Setting Global Logging and Notification Preferences

To see the Log Server status and configuration, click the Log Server icon on the WatchGuard® toolbar and select **Status/Configuration**. The status and configuration information appears. There are three control areas:

Log Files tab
To set the options for rolling your log file.

Reports tab
To schedule regular reports of log entries.

Notification tab
To configure e-mail notification.

Together, these controls set the general configuration for events and notifications.

Log file size and rollover frequency

You can control the log rollover by size or by time. When this rollover occurs, the Log Server closes the current log file and opens a new log file. The closed log file can be used for reports. Copy or move it to a different location to save it for archives.

To find the best rollover size for your company, you must look at:

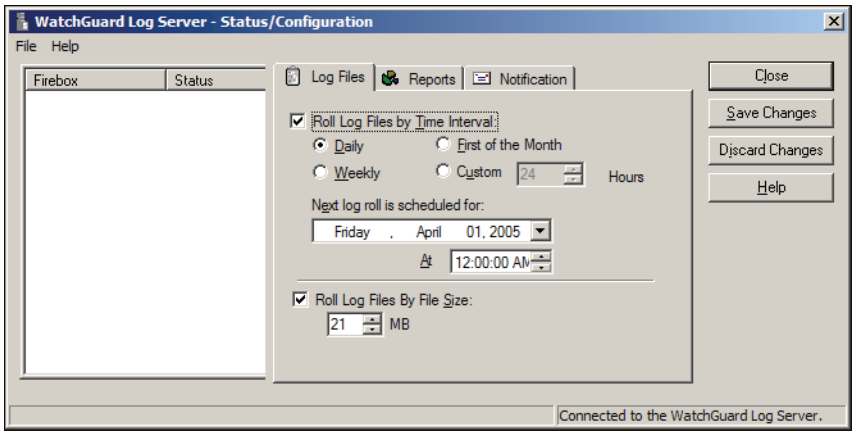
- Storage space that is available
- Number of days you want available
- Size that is best to keep, open, and view
- Number of event types that are recorded
  For example, a small company can get 10,000 entries in two weeks, and a large company with many policies enabled can easily have 100,000 entries in a day.
- Traffic on the Firebox®
- Number of reports to create
  To create a weekly report, it is necessary to have eight or more days of data. This data can be found in more than one log file, if the log files are in the same location.

It is good to monitor the new log files and adjust the configuration as necessary.

Setting when log files rollover

You can control when the log files rollover in the **Log Files** tab in the Log Server configuration interface. You also can manually start a rollover of the current log file. To do this, select **File > Roll current log file** from the **Status/Configuration** window.

1 To set when log files rollover, click the **Log Files** tab.



2 To roll the log file on a time interval, select the **Roll Log Files By Time Interval** check box. Set the time interval. From the **Next Log Roll is Scheduled For** drop-down list, select a date when the log file rolls.

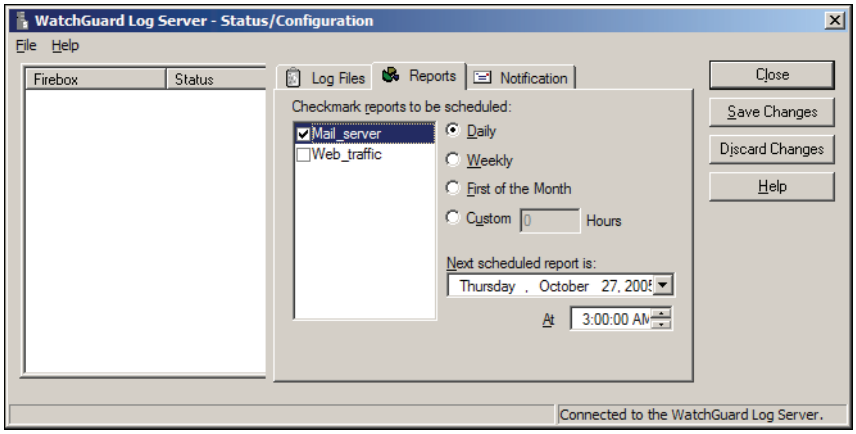
3 To roll the log file based on the size of the log file, select the **Roll Log Files By File Size** check box. Type the maximum size for the log file before the file rolls, or use the spin control to set the number.

4 Click **Save Changes** or **Close**.
The Log Server interface closes and saves your entries. The new configuration starts immediately.
The Log Server restarts automatically.

Scheduling automated reports

If you have created network activity reports using Historical Reports, you can schedule the Log Server component to automate the reports. You first must create a report in Historical Reports, or it does not appear in the Log Server interface.

1 Click the **Reports** tab.



2 Use the radio buttons to set the time interval for reports: daily, weekly, first day of the month, or at a custom time.

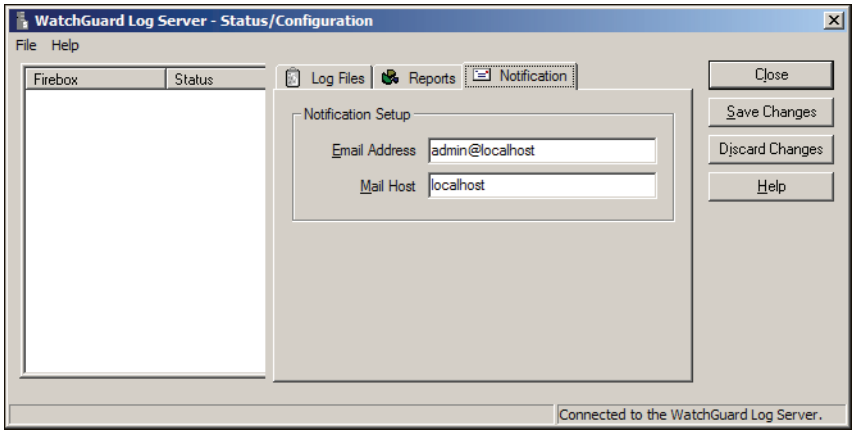
3 From the **Next Scheduled Report** drop-down list, select a date and time for the subsequent scheduled report.

4 Click **Save Changes** or **Close**.
The Log Server interface closes and saves your entries. The new configuration starts immediately.
The Log Server restarts automatically.

Controlling notification

You can configure the Firebox to send an e-mail message when a specified event occurs. Use the **Notification** tab to configure the destination e-mail address.

1 Click the **Notification** tab.



2 Type the e-mail address and the mail host for notification e-mail messages.

Notification e-mail messages have the format firebox_name@[firebox_ip_address]. Make sure that the SMTP server can handle this format.

Consider changing the default values. If the logging host does not resolve to an FQDN, and the receiving MX server does reverse lookups, the e-mail might be discarded.

3 Click **Save Changes** or **Close.**

The Log Server interface closes and saves your entries. The new configuration starts immediately.

The Log Server restarts automatically.

Starting and stopping the Log Server

You can manually stop or start the Log Server:

- To start the Log Server, right-click the Log Server icon on the toolbar and select **Start Service**.
- To stop the Log Server, right-click the Log Server icon on the toolbar and select **Stop Service**.

About Log Messages

WatchGuard® System Manager includes strong and flexible log message tools. An important feature of a good network security policy is to log messages from your security systems, to examine those records frequently, and to keep them in an archive. You can use logs to monitor your network security and activity, identify any security risks, and address them.

The WatchGuard® Firebox X Core and Firebox X Peak send log messages to a shared log management system called the Log Server. They also can send log messages to a syslog server or keep logs locally on the Firebox. You can choose to send logs to either or both of these locations.

You can use Firebox System Manager to log messages in the **Traffic Monitor** tab. For more information, see the "Monitoring Firebox Status" chapter. You also can examine log messages with LogViewer. The log messages are kept in an XML file with a .wgl.xml extension in the WatchGuard directory on the log server. To learn more about the format of log messages, see the "Log Messages" chapter in the *Reference Guide*.

Types of Log Messages

The Firebox® sends four types of log messages. The type appears in the text of the message. The four types of log messages are:

- Traffic
- Alarm
- Event
- Diagnostic

Traffic log messages

The Firebox sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the Firebox.

Alarm log messages

Alarm log messages are sent when an event occurs that triggers the Firebox to do a command. When the alarm condition is matched, the Firebox sends an Alarm log message to the Traffic Monitor and Log Server and then it does the specified action.

You can set some alarm log messages. For example, you can use Policy Manager to configure an alarm to occur when a specified value matches or is more than a threshold. Other alarm log messages are set by the appliance software, and you cannot change the value. For example, the Firebox sends an alarm log message when a network connection on one of the Firebox interfaces fails or when a Denial of Service attack occurs. For more information about alarm log messages, see the *Reference Guide*.

There are eight categories of alarm log messages: System, IPS, AV, Policy, Proxy, Counter, Denial of Service, and Traffic. The Firebox does not send more than 10 alarms in 15 minutes for the same conditions.

Event log messages

The Firebox sends an event log messages because of user activity. Actions that can cause the Firebox to send an event log message include:

- Firebox start up and shut down
- Firebox and VPN authentication
- Process start up and shut down
- Problems with the Firebox hardware components
- Any task done by the Firebox administrator

Diagnostic log messages

Diagnostic log messages include information that you can use to help troubleshoot problems. There are 27 different product components that can send diagnostic log messages. You can select whether the diagnotic log messages appear in Traffic Monitor, as described in “Enabling advanced diagnostics” on page 85.

Log File Names and Locations

The Firebox® sends log messages to a primary or backup Log Server. The default location for the log file is My Documents > My WatchGuard > Shared WatchGuard > logs.

The name of the log file shows:

- If the Firebox has a name, the format of the log file name is `FireboxName-date.wgl.xml`.
- If the Firebox does not have a name, the name of the log files is `FireboxIP-date.wgl.xml`.

Starting LogViewer

LogViewer is the WatchGuard® System Manager tool you use to see the log file data. It can show the log data page by page, or search and display by key words or specified log fields.

1 From WatchGuard System Manager, select **Tools > Logs > LogViewer**.

or
Click the LogViewer icon on the WatchGuard System Manager toolbar. The icon is shown at the left.

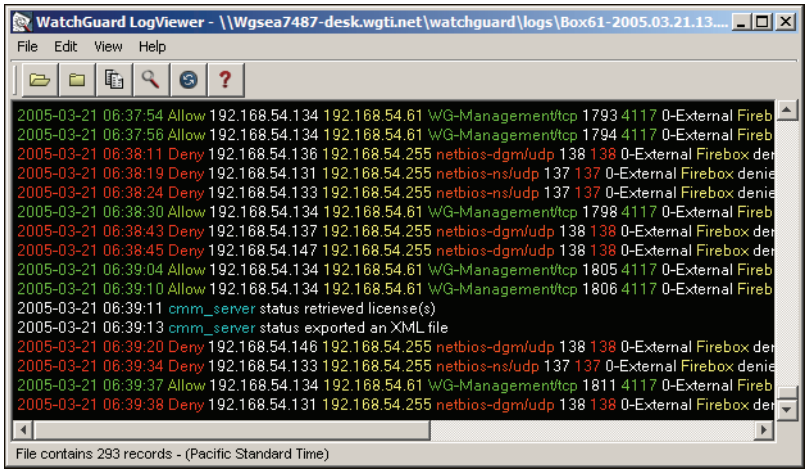
2 From LogViewer, select **File > Open**.

or
Click the Open File icon on the LogViewer toolbar. The icon is shown at the left.

The default location of the logs is My Documents > My WatchGuard > Shared Watchguard > logs.

3 Browse to find the log file and click **Open**.

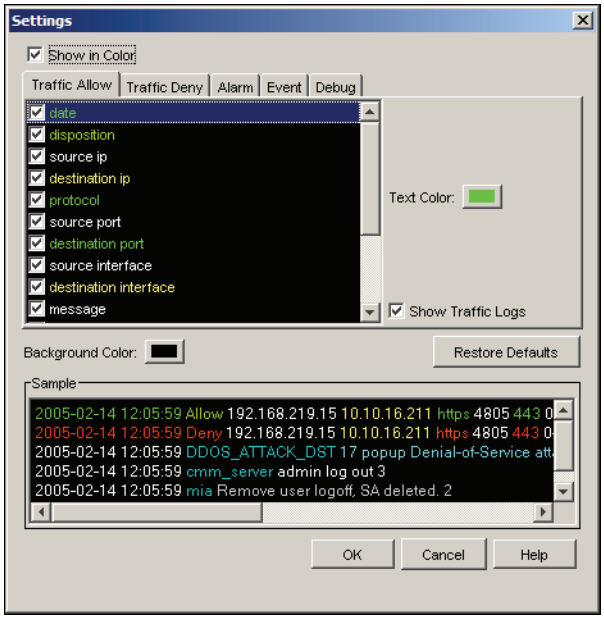
LogViewer shows the log file you selected. A sample appears below.



LogViewer Settings

You can adjust the content and the format of the LogViewer window.

1 From LogViewer, select **View > Settings**.
The Settings dialog box appears.



The **Settings** dialog box has five tabs, each with the same fields. You use these tabs to set properties for the four types of messages that appear in log files: Alarms, Traffic, Event, and Diagnostic.

Show Logs in Color
You can set the messages to appear in different colors based on the type of log message. If color is not enabled, log messages appear as white text on a black background.

Show Columns
For each type of log message, you can select which columns to show in the LogViewer window. Select the check box adjacent to each field to make it appear.

Text Color
Click **Text Color** to set the color for each type of log message.

Background Color
You can set the background color. If the background and text are the same color, you cannot see the text.

Reset Defaults
Click to set the format of the log messages to the default colors.

Sample
Shows a sample log message with format changes.

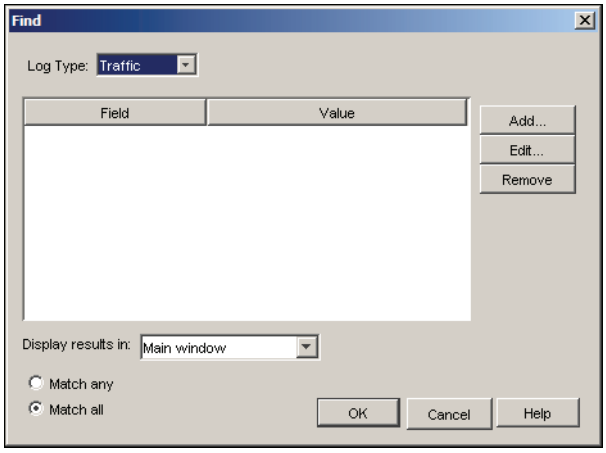
Show logs
This check box is on each tab. If the check box is selected on a tab, the log messages for that type of log are included in the LogViewer display. To clear one type of log message from the display, clear the check box on the tab that matches the log type.

Using LogViewer

Creating a Search Rule

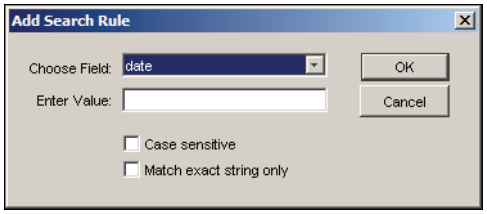
You can create rules to search through the data shown in LogViewer.

1 Select **Edit > Find** (or click the icon with the magnifying glass on it).
The Find dialog box appears.



2 Use the **Log Type** drop-down list to select the type of log message to apply the search rule to. You can select: Traffic, Event, Alarm, Debug, or All.

3 Click on the **Field** column header and select **Add**.
The Add Search Rule dialog box appears.



4 In the **Choose Field** drop-down list, select the field to search.

5 In the **Enter Value** text box, type the text or value to search for.

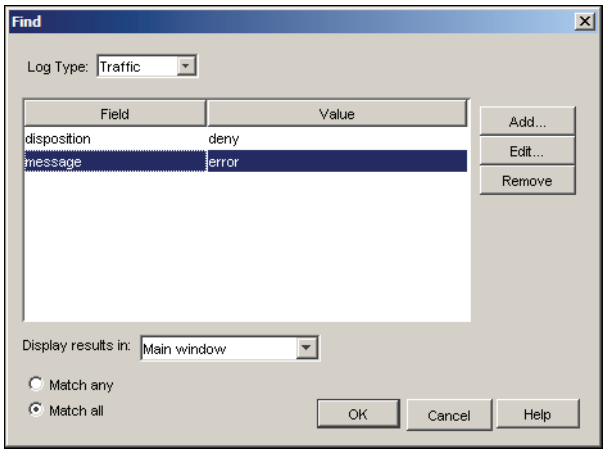
6 If the text you typed in the **Enter Value** text box is case-sensitive, select the **Match Case** check box. To find only entries that match the value precisely, select the **Match exact string only** check box.

7 Click **OK**.

Searching in LogViewer

After you make a search rule, you can use it to search the data shown in LogViewer.

1 Use the **Log Type** drop-down list to select which type of log messages appears in the window.



2 Use the **Display Results** drop-down list to select the method to show the results of the search. The options are:
- *Highlight in main window* — The LogViewer window shows the same log message set, but changes the color of log messages that match the criteria. Use the F3 key to move through specified entries.
- *Main window* — Only the log messages that match the search criteria appear in the primary LogViewer window.
- *New window* - A new window opens to show log messages that match the search criteria.

3 Select from the option:
- *Match any* — Show log messages that match any of the search criteria.
- *Match all* — Show only log messages that match all of the search criteria.

4 Click **OK** to start the search.

Viewing the current log file in LogViewer

You can open the current log file in LogViewer to examine the logs as they are written to the log file. LogViewer automatically updates its display with new log messages at 15-second intervals. If you have a LogViewer search window open with the current log file, it also updates every 15 seconds.

Copying LogViewer data

You can copy log file data from LogViewer to a different tool. Use **copy** to move specified log messages to a different tool.

1 Select the log messages to copy.
Use the Shift key to select a group of entries. Use the Ctrl key to select more than one entry.

2 Select **Edit > Copy**.

3 Paste the data into any text editor.

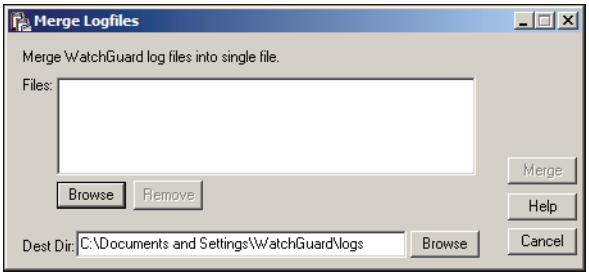
Consolidating log files

You can put together two or more log files into one file. You can then use this file in Historical Reports, LogViewer, or some other tool to examine log data for an extended time interval. To merge more than one log file into one file:

- The log files must be from the same Firebox
- The log messages in the files must be in date and time order
- The log files must be have been created with the same appliance software. You cannot merge a log file created with WFS appliance software with a log file created with Fireware® appliance software, even if they are from the same Firebox.

Right-click the Log Server icon on your Windows toolbar and select **Merge Log Files**. Or, from the Log Server Status/Configuration interface:

1 Click **File > Merge log files.**
The Merge Logfiles dialog box appears.



2 Click **Browse** to find the files to put together.

3 Click **Merge**.
The log files are put together and saved to a new file in the specified directory.

Updating .wgl log files to .xml format

When you migrate from an earlier version of WatchGuard System Manager to WSM 8.3 you can convert log files from .wgl to .xml format. This is also helpful if you manage a mixed network with different versions of WSM. After converting, you can use your WSM 8.3 LogViewer or report tools on log files created with WatchGuard Management System 7.3 or earlier.

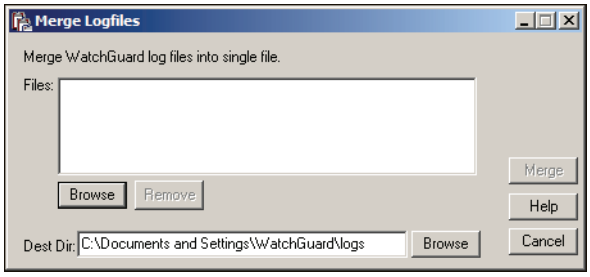
To help you understand the new log structure, or to integrate .xml-format logs into a third-party application, see the following Advanced FAQ. It gives an XML schema and Document Type Definition (DTD) for the new WatchGuard log file:
https://www.watchguard.com/support/AdvancedFaqs/wsm8_xmlschema.asp

When you convert a log file from .wgl to .xml:

- The XML file is usually smaller than the .wgl file.
- If you open the new XML file in an XML editor, you can see some duplicate entries. This is a function of the way Historical Reports made reports in WSM 7.3 and earlier. It does not cause problems in LogViewer or in Historical Reports for WSM 8.3.

To convert a log file from .wgl to .xml:

1 Right-click the Log Server icon on your Windows desktop tray and select **Merge Log Files.**
The Merge Logfiles dialog box appears. This dialog box controls merges, and also updates, of log files.



2 Click **Browse** to find the location of the logfile.wgl to convert to XML. If you select more than one log file at one time, the utility converts all of the files you select and puts them together into one file. The new file has an .xml format.

3 Click **Merge**.
The utility converts the log file and saves it to the specified folder.

CHAPTER 8

Network Setup and Configuration

When you install the Firebox® in your network and complete the Quick Setup Wizard, you have a basic configuration file. You then use Policy Manager to make a new configuration file or to change the one you made with the Quick Setup Wizard.

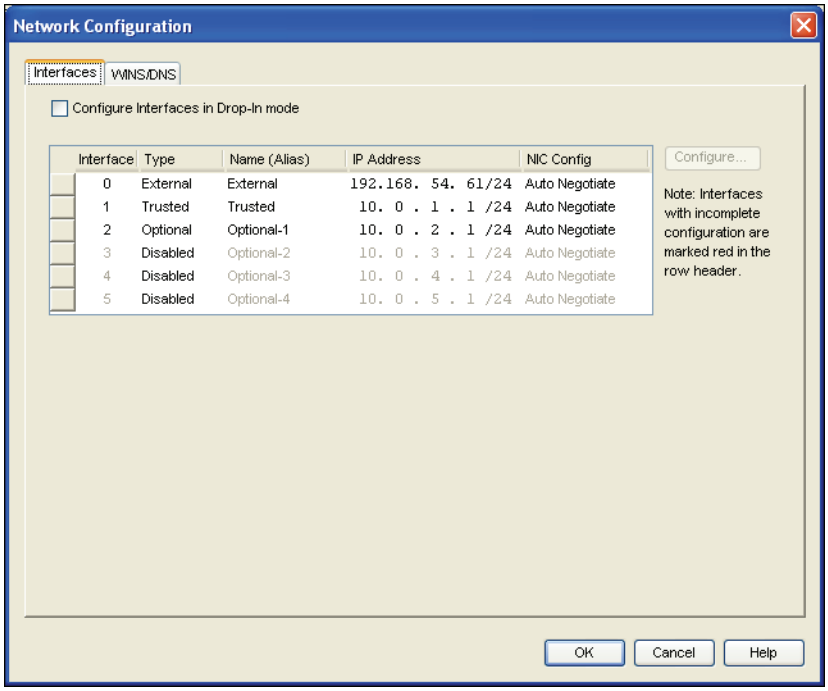
If you are new to network security, we recommend that you do all the procedures in this chapter to make sure you configure all the components of your network. In this chapter, you learn how to use Policy Manager to:

- Configure the Firebox interfaces
- Configure Multi-WAN support
- Add a secondary network
- Add DNS and WINS server information
- Configure Dynamic DNS
- Configure network and host routes
- Set Firebox interface speed and duplex
- Configure related hosts

You can also use Policy Manager to configure up to four Firebox interfaces as external, or wide area network (WAN), interfaces. You can control the flow of traffic through multiple WAN interfaces to share the load of outgoing traffic.

Changing Firebox Interface IP Addresses

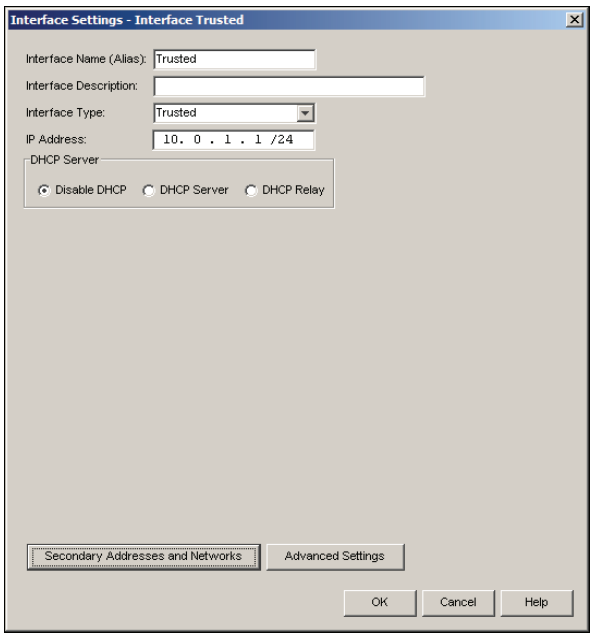
1 From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.


Network Configuration
Interfaces
WINS/DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
0 External External 192.168. 54. 61/24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 Disabled Optional-2 10. 0 . 3 . 1 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
Configure...
Note: Interfaces with incomplete configuration are marked red in the row header.
OK
Cancel
Help

2 Select the interface you want to configure. Click **Configure**.
The Interface Settings dialog box appears.

3 (Optional) Type a description of the interface in the **Interface Description** field.

4 You can change the interface type from the **Interface Type** drop-down list.



5 You can change the interface IP address. Type the IP address in slash notation.
When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

6 If you are configuring a trusted or optional interface, select **Disable DHCP**, **DHCP Server**, or **DHCP Relay**.
See "Configuring the Firebox as a DHCP server" for the DHCP server option, and see "Configuring a DHCP relay" on page 99 for the DHCP relay option. If you are configuring the external interface, see "Configuring the external interface" on page 100.

7 Click **OK**.

Configuring the Firebox as a DHCP server

Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that makes it easier to control a large network. A computer you configure as the DHCP server automatically gives IP addresses to the computers on your network. You set the range of addresses. You can configure the Firebox® as a DHCP server for networks behind the Firebox.

If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.

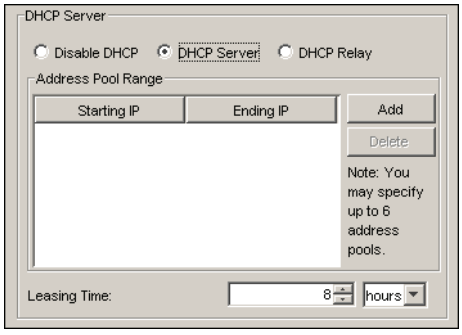
1 Select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Select the trusted or an optional interface.

3 Click **Configure** and select **DHCP Server**.

4 To add an IP address range, click **Add** and type the first and last IP addresses.
You can configure a maximum of six address ranges.

5 Use the arrow buttons to change the **Default Lease Time**.
This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client sends data to the DHCP server to get a new lease.



Configuring a DHCP relay

One method to get IP addresses for the computers on the Firebox trusted or on an optional network is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different location than the DHCP client. When the Firebox gets the reply, it sends it to the computers on the Firebox trusted or optional network.

1 Select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Select the trusted or an optional interface.

3 Click **Configure** and click **DHCP Relay**.

4 Type the IP address of the DHCP server in the related field. Make sure to add a route to the DHCP server, if necessary.

5 Click **OK.** You must restart the Firebox to complete the change.

Configuring the external interface

The Firebox can get a dynamic IP address for the external interface with Dynamic Host Configuration Protocol (DHCP) or PPPoE (Point-to-Point Protocol over Ethernet). With DHCP, the Firebox uses a DHCP server that is controlled by your Internet Service Provider (ISP) to get an IP address, gateway, and net-mask. With PPPoE, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. Fire-ware® supports unnumbered and static PPPoE.

Note

If you configure more than one interface as an external interface, only the lowest-order external interface can serve as an IKE gateway or an IPSec tunnel endpoint. If this interface is down, all IPSec tunnels to and from the Firebox will not operate.

Using a static IP address

1 From the **Interface Settings** dialog box, select **Static**.

2 Type the IP address of the default gateway.

3 Click **OK**.

Using PPPoE

Some ISPs assign their IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE expands a standard dial-up connection to add some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

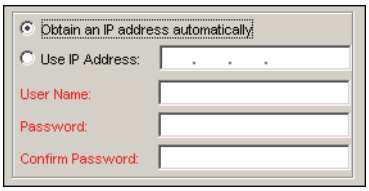
If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox before it can send traffic through the external interface.

1 From the **Interface Settings** dialog box, select **PPPoE**.

2 Select one of the two options:
- Get an IP address automatically
- Use IP address (supplied by your Internet Service Provider)

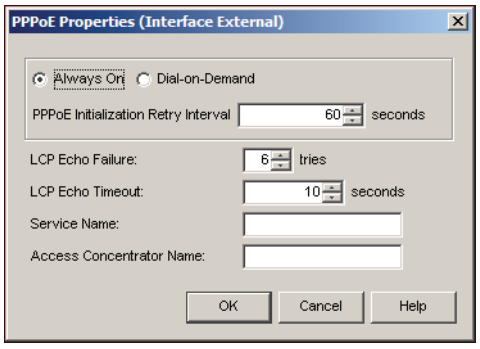
3 If you selected **Use IP Address**, enter the IP address in the text box to the right.

4 Type the **User Name** and **Password**. You must type the password two times.
Frequently, ISPs use the e-mail address format for user names, such as *myname@ispdomain.net*.



5 Click **Property** to configure PPPoE parameters.
The PPPoE parameters dialog box appears. Your ISP can tell you if it is necessary to change the time-out or LCP values.

6 Use the radio buttons to select when the Firebox connects with the PPPoE server.
- **Always On** — The Firebox keeps a constant PPPoE connection. It is not necessary that network traffic go through the external interface.
- **Dial-on-Demand** — The Firebox connects to the PPPoE server only when it gets a request to send traffic to an IP address on the external interface. If your ISP regularly resets the connection, select Dial-on-Demand. If you do not select Dial-on-Demand, you must manually restart the Firebox each time the connection resets.



7 In the **PPPoE Initialization Retry Interval** field, use the arrows to set the number of seconds that PPPoE tries to initialize before it times out.

8 In the **LCP echo failure** field, use the arrows to set the number of failed LCP echo requests allowed before the PPPoE connection is considered inactive and closed.

9 In the **LCP echo timeout** field, use the arrows to set the length of time, in seconds, that the response to each echo time-out must be received.

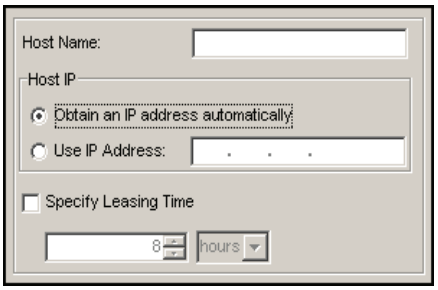
10 (Optional) In the **Service Name** field, type a PPPoE service name. This is either an ISP name or a class of service that is configured on the PPPoE server. Usually, this option is not used. Use this field only if there is more than one access concentrator or you know that you must use a specified service name.

11 (Optional) In the **Access Concentrator Name** field, enter the name of a PPPoE access concentrator, also known as a PPPoE server. Usually, this option is not used. Use it only if you know there is more than one access concentrator.

Using DHCP

1 From the **Interface Settings** dialog box, select **DHCP**.

2 If your DHCP server makes you use an optional identifier in your DHCP exchange, type this identifier in the **Host Name** text box.



3 Under **Host IP**, select the **Obtain an IP address automatically** check box if you want DHCP to assign an IP address to the Firebox. If you want to manually assign an IP address and use DHCP just to give this assigned address to the Firebox, select the **Use IP address** check box and enter the IP address in the adjacent field.

4 IP addresses assigned by a DHCP server have a one-day lease, which means the address is valid for one day. If you want to change the leasing time, select the **Specify Leasing Time** check box and select the value in the fields below the check box.

About Multiple WAN Support

Fireware® appliance software gives you the option to configure multiple external interfaces (up to four), each on a different subnet. This allows you to connect the Firebox® to more than one Internet Service Provider (ISP). As soon as you configure a second external interface, multiple WAN support is automatically enabled with multi-WAN in round robin order set as the default. There are three options to control which interface outgoing packets use.

Note that:

- If you have a policy configured with an individual external interface alias in its configuration, you must change the configuration to use the alias "Any-External".
- If you use the multiple WAN feature, map your company's Fully Qualified Domain Name to the external interface IP address of the lowest order. If you add a multi-WAN Firebox to your Management Server configuration, you must add the Firebox using its lowest-ordered external interface to identify it.
- You cannot use 1-to-1 NAT in a multiple WAN configuration. If you have a public SMTP server behind your Firebox, you must set up a static NAT rule to allow access to your public SMTP e-mail server. Then, you can set up multiple MX records, one for each external Firebox interface.
- If you have a multiple WAN configuration, you cannot use the policy-based, dynamic NAT **Set Source IP** option. Use the **Set Source IP** option only when your Firebox uses a single external interface.
- Multiple WAN support does not apply to branch office or Mobile User VPN traffic. Branch office and Mobile User VPN traffic always uses the first external interface configured for the Firebox. RUVPN with PPTP operates correctly in a multiple WAN configuration.
- The multiple WAN feature is not supported in drop-in mode.

About multi-WAN in round robin order

If you select "round robin" order, you can share the load of outgoing traffic among external interfaces like this:

- The first host, with IP address x.x.x.x, sends an HTTP request to the Internet. The packets in this session are sent through the lowest number external interface.
- The second host, with IP address y.y.y.y, sends an HTTP request to the Internet. The packets in this session are sent through the external interface with the second higher number.
- The third host, with IP address z.z.z.z, sends an HTTP request to the Internet. The packets in this session are sent through the lowest number external interface (if there are only two external interfaces configured) or the third higher number external interface.
- As each host initiates a connection, the Firebox cycles through external interfaces using the pattern explained above.

Note

If you use multi-WAN in round-robin mode, it is possible to set up round-robin DNS with your DNS provider to do load-balancing among more than one external interface.

About WAN Failover

This option is also used only on outgoing traffic. If you select this option, the lowest number external interface configured in your list becomes the primary external interface. All other external interfaces are backup external interfaces. The Firebox sends all outgoing traffic to the primary external interface. If the primary external interface is not active, the Firebox sends traffic to the first backup interface.

The Firebox monitors the status of the primary external interface with two procedures. It checks the physical link status of the interface. It also pings the IP address or domain name of an external host that you configure for each interface each 20 seconds. If three pings to this host fail, the Firebox fails over to the subsequent configured external interface.

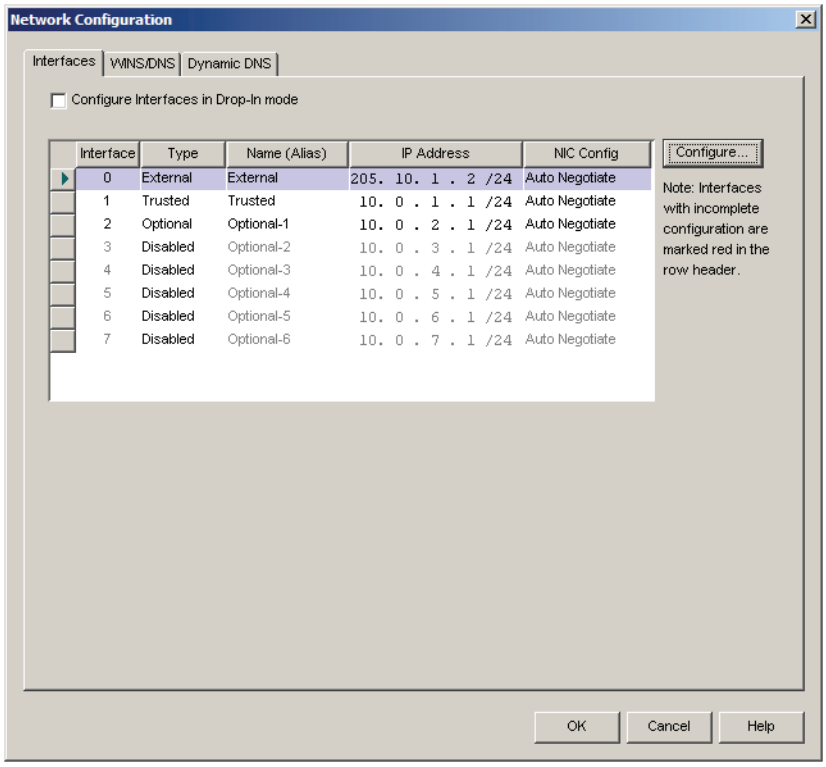
When the Firebox detects that the primary external interface is active again, it automatically starts to send new connections to the primary external interface.

About multi-WAN with the routing table

When you select the routing table option for your multi-WAN configuration, the Firebox uses the routes set in its internal routing table to send packets through the correct external interface. You can set up network or host routes in Policy Manager and the Firebox will examine these routes to see if a packet is to be sent to a specified interface. If the Firebox does not find a specified route, then the Firebox uses the first default route in its routing table. If the Firebox is configured to use dynamic routing, it sends traffic based on the dynamic information recorded in its routing table. To see the routing table on the Firebox, connect to Firebox System Manager and select the **Status** tab.

Configuring multiple WAN support

1 From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.

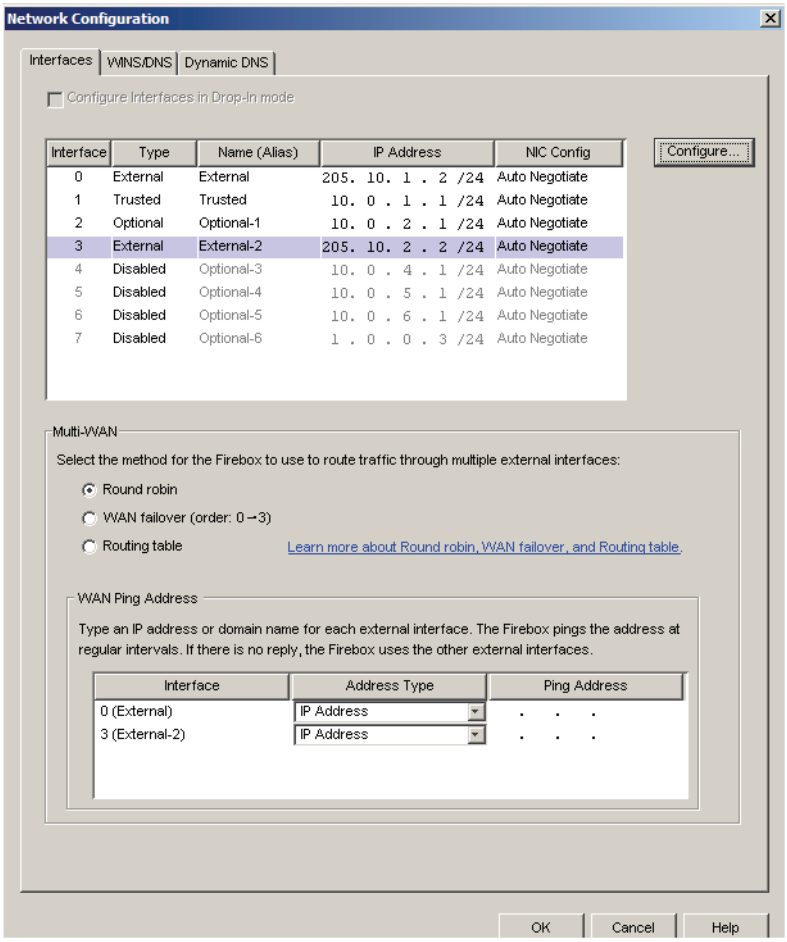

Network Configuration
Interfaces
WINS/DNS
Dynamic DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
0 External External 205. 10. 1 . 2 /24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 Disabled Optional-2 10. 0 . 3 . 1 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
6 Disabled Optional-5 10. 0 . 6 . 1 /24 Auto Negotiate
7 Disabled Optional-6 10. 0 . 7 . 1 /24 Auto Negotiate
Configure...
Note: Interfaces with incomplete configuration are marked red in the row header.
OK
Cancel
Help

2 Select the interface to configure as external and click **Configure**. Select **External** from the **Interface Type** drop-down list to activate the dialog box. Type an interface name and description.
You must have a minimum of two external network interfaces configured before you can see and configure multi-WAN settings.

3 Type the IP address and default gateway for the interface. Click **OK**.

When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

After you configure a second external interface, multiple WAN configuration options appear in the Network Configuration dialog box.


Network Configuration
Interfaces
WINS/DNS
Dynamic DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
Configure...
0 External External 205. 10. 1 . 2 /24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 External External-2 205. 10. 2 . 2 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
6 Disabled Optional-5 10. 0 . 6 . 1 /24 Auto Negotiate
7 Disabled Optional-6 1 . 0 . 0 . 3 /24 Auto Negotiate
Multi-WAN
Select the method for the Firebox to use to route traffic through multiple external interfaces:
Round robin
WAN failover (order: 0→3)
Routing table
Learn more about Round robin, WAN failover, and Routing table.
WAN Ping Address
Type an IP address or domain name for each external interface. The Firebox pings the address at regular intervals. If there is no reply, the Firebox uses the other external interfaces.
Interface
Address Type
Ping Address
0 (External)
IP Address
3 (External-2)
IP Address
OK
Cancel
Help

4 Select the procedure you want to use to control traffic among multiple external interfaces.

These three procedures are described above.

5 In the **WAN Ping Address** dialog box, double-click in the **Ping Address** column to add an IP address or domain name for each external interface. We recommend that you use the IP address of a computer external to your organization.

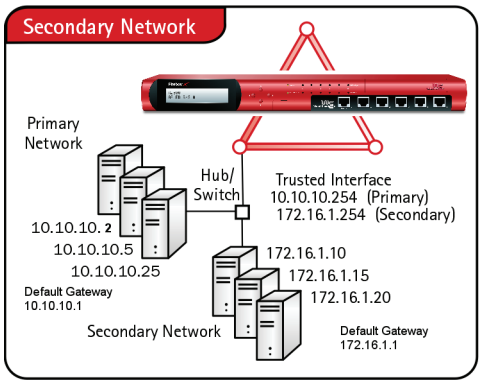
When an external interface is active, the Firebox pings the IP address or domain name you set here each 20 seconds to see if the interface is operating correctly. If there is no response after three pings, the Firebox starts to use the subsequent configured external interface. It then starts to ping the WAN ping address you set for that interface to check for connectivity.

6 Click **OK**. Save your changes to the Firebox.

Adding Secondary Networks

A secondary network is a network that shares one of the same physical networks as one of the Firebox® interfaces. When you add a secondary network, you make (or add) an IP alias to the interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network tells the Firebox that there is one more network on the Firebox interface.

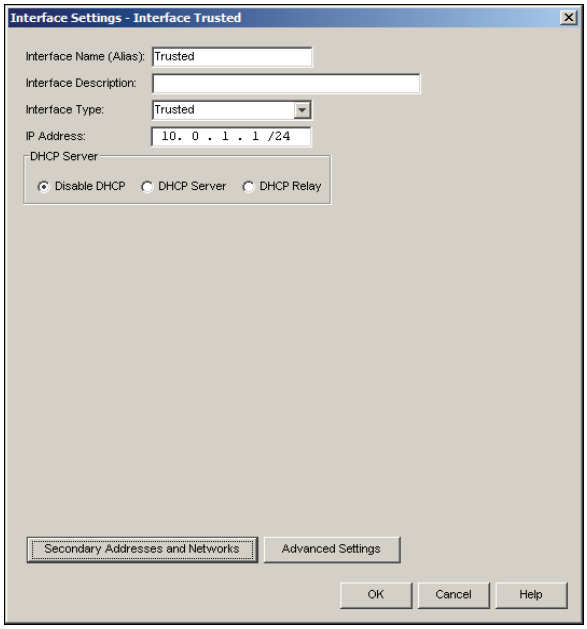
If your Firebox is configured with a static IP address, you can add an IP address on the same subnet as your primary external interface as a secondary network. You can then configure static NAT for more than one of the same type of server. For example, configure an external secondary network with a second public IP address if you have two public SMTP servers and you want to configure a static NAT rule for each.



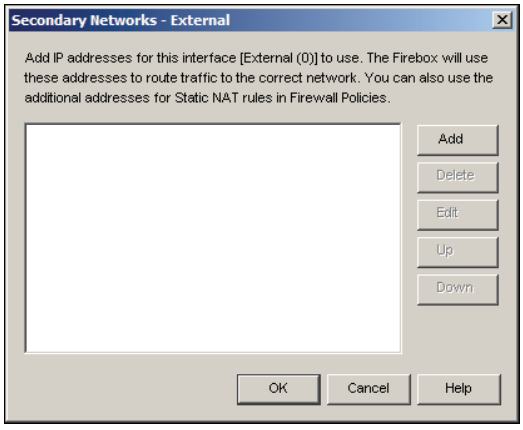
To use Policy Manager to configure a secondary network:

1 Select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Select the interface for the secondary network and click **Configure**.
The Interface Settings dialog box appears.



3 Click **Secondary Addresses and Networks**.
The Secondary Networks dialog box appears.


Secondary Networks - External
Add IP addresses for this interface [External (0)] to use. The Firebox will use these addresses to route traffic to the correct network. You can also use the additional addresses for Static NAT rules in Firewall Policies.
Add
Delete
Edit
Up
Down
OK
Cancel
Help

4 Click **Add**. Type an unassigned IP address from the secondary network.
When you type IP addresses, type all the numbers and the stops. Do not use the TAB or arrow key.

5 Click **OK**. Click **OK** again.

Note

Be careful to add secondary network addresses correctly. Policy Manager does not tell you if the address is correct. We recommend that you do not create a subnet as a secondary network on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network cannot operate correctly.

Adding WINS and DNS Server Addresses

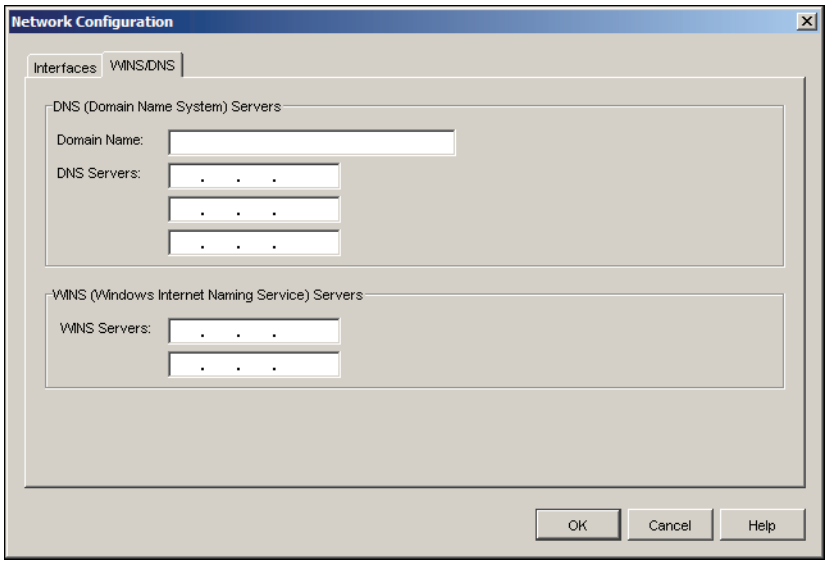
A number of the features of the Firebox® must have shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses. These features include DHCP and Remote User VPN. Access to these servers must be available from the trusted interface of the Firebox.

This information is used for two purposes:

- The Firebox uses the DNS server shown here to resolve names to IP addresses for IPSec VPNs and for the spamBlocker, GAV and IPS features to operate correctly.
- The WINS and DNS entries are used by DHCP clients on the trusted or optional networks, MUVPN users, and PPTP RUVPN users to resolve DNS queries.

Make sure that you use only an internal WINS and DNS server for DHCP and RUVPN. This helps to make sure that you do not make policies that have configuration properties that prevent users from connecting to the DNS server.

1 From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab.
The information on the WINS/DNS tab appears.



2 Type the primary and secondary addresses for the WINS and DNS servers. You can also type a domain suffix in the **Domain Name** text box for a DHCP client to use with unqualified names such as "kunstler_mail".

Configuring Dynamic DNS

You can register the external IP address of the Firebox® with a dynamic Domain Name Server (DNS) service. A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives your Firebox a new IP address. The Firebox supports one Dynamic DNS provider: DynDNS. For more information on Dynamic DNS, log on to the DynDNS web site:

http://www.dyndns.com

Note

WatchGuard® is not affiliated with DynDNS.

Creating a DynDNS account

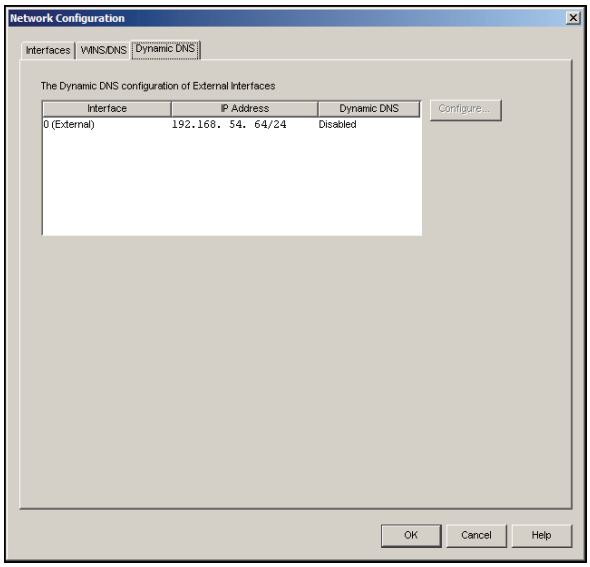
To set up your account, go to this web site:

http://www.dyndns.com

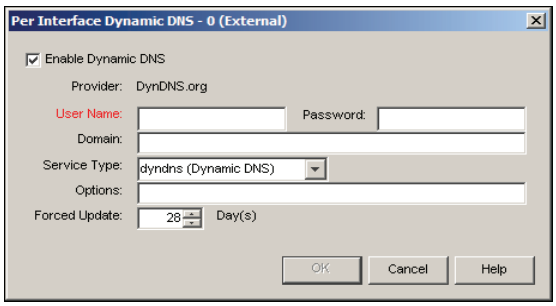
Use the instructions on the DynDNS web site to activate your account. You must do this before you configure the Firebox for Dynamic DNS.

Setting up the Firebox for Dynamic DNS

1 From Policy Manager, select **Network > Configuration**. Click the **Dynamic DNS** tab.
The information on the Dynamic DNS tab appears.



2 Select the external interface you want to configure Dynamic DNS for and click **Configure**.
The Per Interface Dynamic DNS dialog box appears.



3 To enable Dynamic DNS, select the **Enable Dynamic DNS** check box.

4 Type the user name, password, and domain name you used to set up your Dynamic DNS account.

5 In the **Service Type** drop-down list, select the system to use for this update:

- **dyndns** sends updates for a Dynamic DNS host name.
- **statdns** sends updates for a Static DNS host name.
- **custom** sends updates for a Custom DNS host name.

For more information on each option, see http://www.dyndns.com/services/.

6 In the **Options** field, you can type any of the options shown below. You must type an "&" character before and after each option you add. If you add more than one option, you must separate the options with the "&" character. For example: &backmx=NO&wildcard=ON&

mx=mailexchanger
backmx=YES|NO
wildcard=ON|OFF|NOCHG
offline=YES|NO

For more information on options, see:
http://www.dyndns.com/developers/specs/syntax.html

7 Use the arrows to set a time interval, in days, to force an update of the IP address.

Configuring Routes

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

The Firebox® lets you create static routes to send traffic from its interfaces to a router. The router can then send the traffic to the correct destination from the specified route. If you do not add a route to a remote network, all traffic to that network is sent to the Firebox default gateway.

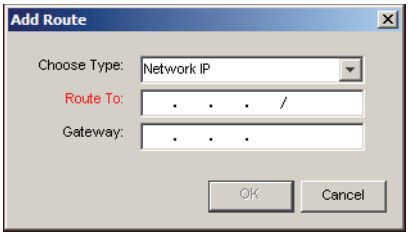
The WatchGuard® Users Forum is also a good source of data about network routes and routers. Use your LiveSecurity service to find more information.

Adding a network route

Add a network route if you have a full network behind a router on your local network. Type the network IP address, with slash notation.

1 From Policy Manager, select **Network > Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.



3 Select **Network IP** from the drop-down list.

4 In the **Route To** text box, type the network address. Use slash notation.
For example, type 10.10.1.0/24. A /24 network always has a zero for the last octet.

5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is on one of the same networks as the Firebox.

6 Click **OK** to close the **Add Route** dialog box.
The Setup Routes dialog box shows the configured network route.

7 Click **OK** again to close the **Setup Routes** dialog box.

Adding a host route

Add a host route if there is only one host behind the router or you want traffic to go to only one host. Type the IP address of that specified host, with no slash notation.

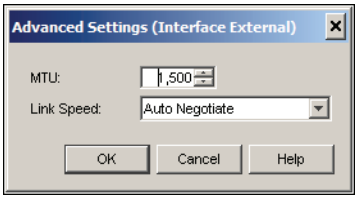
1 From Policy Manager, select **Network > Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.
3 Select **Host IP** from the drop-down list.
4 In the **Route To** text box, type the host IP address.
5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is on one of the same networks as the Firebox.
6 Click **OK** to close the **Add Route** dialog box.
The Setup Routes dialog box shows the configured host route.
7 Click **OK** again to close the **Setup Routes** dialog box.

Setting Firebox Interface Speed and Duplex

You can configure the speed and duplex parameters for Firebox® interfaces to automatic or manual configuration. We recommend you set the speed and duplex parameters to match the device the Firebox connects to. Use the manual configuration option when you must override the automatic Firebox interface parameters to operate with other devices on your network.

1 Select **Network > Configuration**. Click the interface you want to configure, and then click **Configure**.
2 Click **Advanced Settings**.
The Advanced Settings dialog box appears.



3 From the **MTU** value control, select the maximum packet size, in bytes, that can be sent through the interface.
If you use PPPoE, you must change this value to 1492, or the MRU supported by your ISP. If you do not use PPPoE, we do not recommend that you change the MTU value.
4 From the **Link Speed** drop-down list, select **Auto Negotiate** if you want the Firebox to select the best network speed. You can also select one of the half-duplex or full-duplex speeds that you know is compatible with your equipment.
5 Click **OK** to close the **Advanced Settings** dialog box. Click **OK** again to close the **Network Configuration** dialog box.

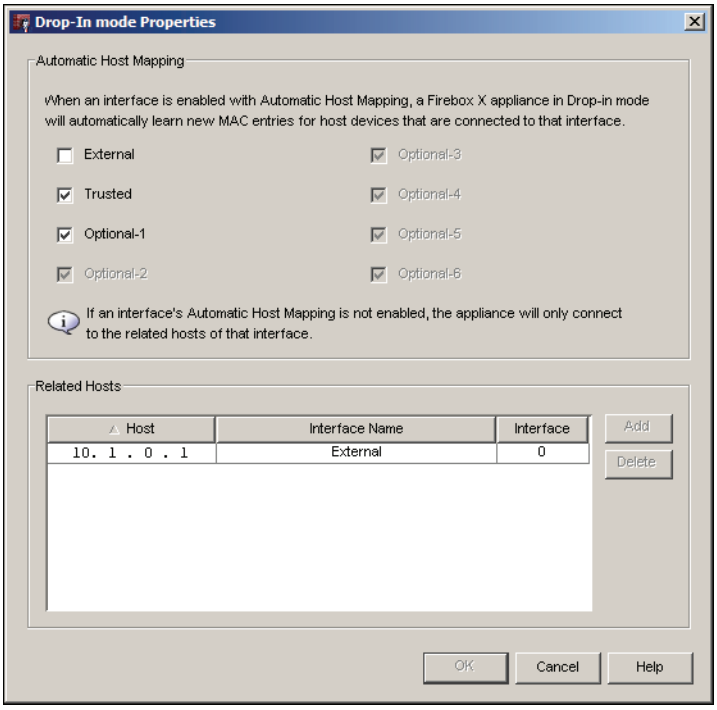
Configuring Related Hosts

In a drop-in configuration, the Firebox® is configured with the same IP address on each interface. The drop-in configuration mode distributes the network's address range across the Firebox interfaces. Related hosts are sometimes required when you have configured your Firebox in drop-in mode and automatic host mapping is not functioning correctly. This sometimes happens because of interference with the Firebox trying to discover devices on an interface. When this occurs, turn off automatic host mapping and add related host entries for computers that share a network address with the Firebox. This creates a static routing relationship between the related host IP address and the interface designated

for that IP address. When there are problems with dynamic/automatic host mapping, you must use related host entries.

1 From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Click **Properties**.
The Drop-In Mode Properties dialog box appears.



3 Disable automatic host mapping on any interface on which automatic host mapping is not operating correctly.

4 Click **Add**. Type the IP address of the computer for which you want to build a static route from the Firebox.

5 Click on the **Interface Name** column to select the interface the related host is connected to

6 After you have added all related host entries, click **OK**. Save the configuration to the Firebox.

CHAPTER 9

Working with Firewall NAT

Network Address Translation (NAT) was first developed as a solution for organizations that could not get enough registered IP network numbers from Internet Address Registrars for their increasing population of hosts and networks.

NAT is generically used to describe any of several forms of IP address and port translation. At its most basic level, NAT changes the IP address of a packet from one value to a different value. The primary purposes of NAT are to increase the number of computers that can operate off a single publicly routable IP address, and to hide the private IP addresses of hosts on your LAN.

There are different ways to use NAT. WatchGuard® System Manager supports three different forms of NAT.

Dynamic NAT

Dynamic NAT is also known as IP masquerading. The Firebox® can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network. Dynamic NAT is generally used to hide the IP addresses of internal hosts when they get access to public services.

1-to-1 NAT

1-to-1 NAT binds hosts behind your optional or trusted networks to external IP addresses. This type of NAT is used to give external computers access to your public, internal servers.

Static NAT for a policy

Also known as port forwarding, you configure static NAT when you configure policies, as described in "Configuring Policies," on page 65. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall.

It is possible that, in your configuration, you use more than one type of NAT. You can apply NAT as a general firewall setting, or as a setting in a policy. Note that firewall NAT settings do not apply to BOVPN or MUVPN policies.

Using Dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the Firebox®. Outside the Firebox, you see only the IP address of the Firebox on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network. With Dynamic NAT, all connections must start from behind the Firebox. Malicious hosts cannot start connections to the computers behind the Firebox when the Firebox is configured for dynamic NAT.

In most networks, the recommended security policy is to apply NAT to all outgoing packets. With Fireware®, dynamic NAT is enabled by default in the **Network > NAT** dialog box. It is also enabled by default in each policy you create. You can override the firewall setting for Dynamic NAT in your individual policies.

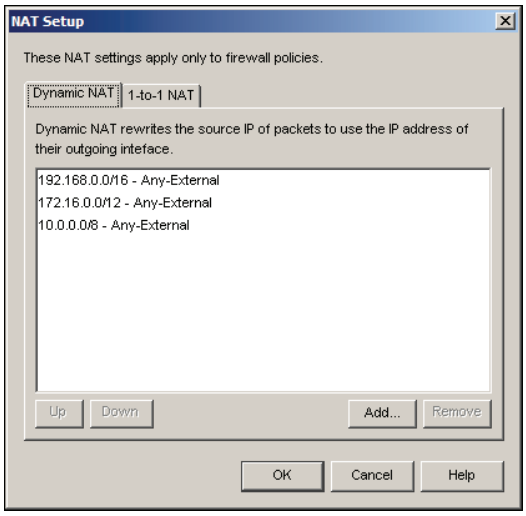
Adding firewall dynamic NAT entries

The default configuration of dynamic NAT enables dynamic NAT from all private IP addresses to the external network. The default entries are:

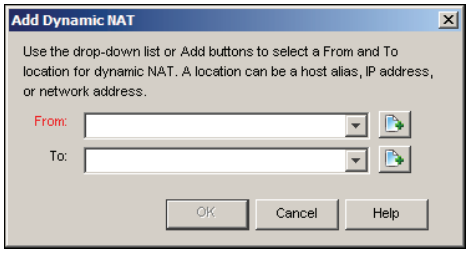
- 192.168.0.0/16 - Any-External
- 172.16.0.0/12 - Any-External
- 10.0.0.0/8 - Any-External

These three network addresses are the private networks reserved by the Internet Engineering Task Force (IETF) and usually are used for the IP addresses on LANs. To enable dynamic NAT for private IP addresses other than these, you must add an entry for them. The Firebox applies the dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list. We recommend that you put the rules in a sequence that matches the volume of traffic the rules apply to.

1 From Policy Manager, select **Network > NAT**.
The NAT Setup dialog box appears.



2 On the **Dynamic NAT** tab of the **NAT Setup** dialog box, click **Add**.
The Add Dynamic NAT dialog box appears.


Add Dynamic NAT
Use the drop-down list or Add buttons to select a From and To location for dynamic NAT. A location can be a host alias, IP address, or network address.
From:
To:
OK
Cancel
Help

3 Use the **From** drop-down list to select the source of the outgoing packets.
For example, use the trusted host alias to enable NAT from all of the trusted network. For more information on built-in Firebox aliases, see "Working with Aliases" on page 73.

4 Use the **To** drop-down list to select the destination of the outgoing packets.

5 To add a host or a network IP address, click the **Add Device** button shown at the right. Use the drop-down list to select the address type. Type the IP address or the range. You must type a network address in slash notation.

When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

6 Click **OK**.
The new entry appears in the Dynamic NAT Entries list.

Reordering dynamic NAT entries

To change the sequence of the dynamic NAT entries, select the entry to change. Then click **Up** or **Down**.

You cannot change a dynamic NAT entry. If a change is necessary, you must delete the entry with **Remove**. Use **Add** to enter it again.

Policy-based dynamic NAT entries

With this type of NAT, the Firebox uses the primary IP address of the outgoing interface for the outgoing packets for this policy. Each policy has dynamic NAT enabled by default, which uses the global dynamic NAT table. You can disable dynamic NAT for all traffic in a policy.

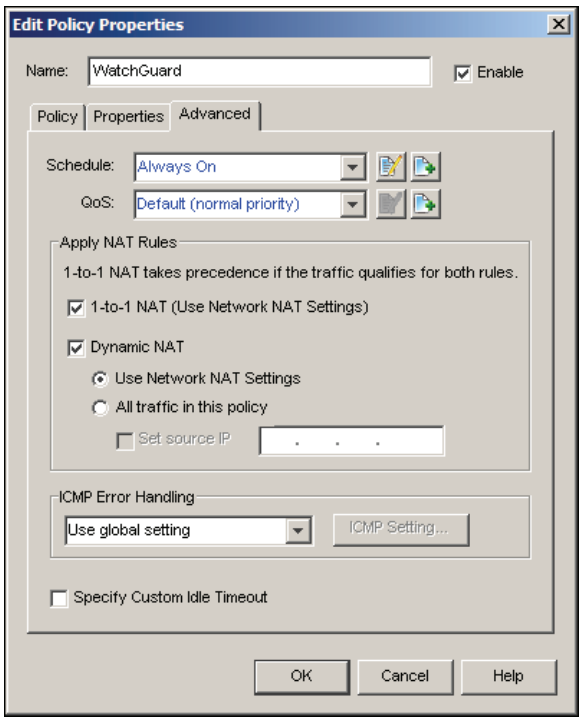
Disabling policy-based dynamic NAT

1 From Policy Manager, right-click a policy and select **Edit**.
The Edit Policy Properties window appears.

2 Click the **Advanced** tab.

3 Clear the check box in front of **Dynamic NAT** to turn NAT off for the traffic this policy controls.

4 Click **OK**. Save the change to the Firebox.



Using 1-to-1 NAT

When you enable 1-to-1 NAT, the Firebox® changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses. You can configure up to 64 different 1-to-1 NAT addresses. This allows you to configure a 1-to-1 NAT rule for a single /26 network, or a total of 64 IP addresses among all 1-to-1 NAT rule entries. A 1-to-1 NAT rule always has precedence over dynamic NAT.

1-to-1 NAT is frequently used when you have a group of internal servers with private IP addresses that must be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers. You do not have to change the IP address of your internal servers. When you have a group of similar servers (for example, a group of e-mail servers), 1-to-1 NAT is easier to configure than static NAT for the same group of servers.

To understand how to configure 1-to-1 NAT, we give this example:

Company ABC has a group of five privately addressed e-mail servers behind the trusted interface of their Firebox X Peak. These addresses are:

10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
10.1.1.5

Company ABC selects five public IP addresses from the same network address as the external interface of their Firebox, and creates DNS records for the e-mail servers to resolve to. These addresses are:

50.1.1.1

50.1.1.2
50.1.1.3
50.1.1.4
50.1.1.5

Company ABC configures a 1-to-1 NAT rule for their e-mail servers. The 1-to-1 NAT rule builds a static, bi-directional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.1.1.1 <--> 50.1.1.1
10.1.1.2 <--> 50.1.1.2
10.1.1.3 <--> 50.1.1.3
10.1.1.4 <--> 50.1.1.4
10.1.1.5 <--> 50.1.1.5

When the 1-to-1 NAT rule is applied, the Firebox creates the bi-directional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.

Defining a 1-to-1 NAT rule

In each 1-to-1 NAT policy you can configure a host, a range of hosts, or a subnet. You must also configure:

Interface
The name of the Firebox® Ethernet interface on which 1-to-1 NAT is applied. The Firebox will apply 1-to-1 NAT for packets sent in to, and out of, the interface. In our example above, the rule is applied to the external interface.

NAT base
When you configure a 1-to1 NAT policy, you configure the policy with a "from" and a "to" range of IP addresses. The NAT base is the first available IP address in the "to" range of addresses. The NAT base IP address is the address that the real base IP address changes to when the 1-to-1 NAT is applied. In our example above, the NAT base is 50.1.1.1.

Real base
When you configure a 1-to-1 NAT policy, you configure the policy with a "from" and a "to" range of IP addresses. The Real base is the first available IP address in the "from" range of addresses. It is the IP address assigned to the physical Ethernet interface of the computer to which you will apply the 1-to-1 NAT policy. When packets from a computer with a real base address go through the interface specified, the 1-to-1 action is applied. In our example above, the Real base is 10.1.1.1.

Number of hosts to NAT (for ranges only)
The number of IP addresses in a range to which the 1-to-1 NAT rule applies. The first real base IP address is translated to the first NAT Base IP address when 1-to-1 NAT is applied. The second real base IP address in the range is translated to the second NAT base IP address when 1-to-1 NAT is applied. This is repeated until the "Number of hosts to NAT" is reached. In our example above, the number of hosts to apply NAT to is five.

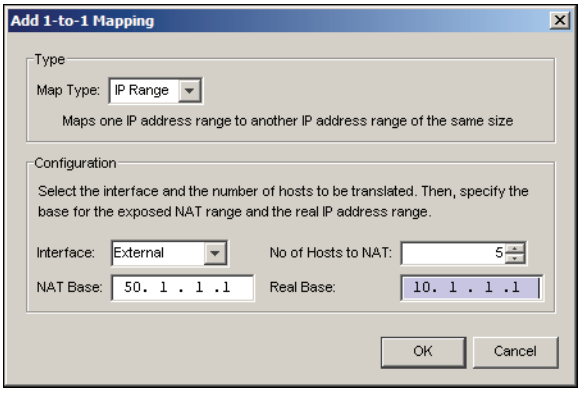
You can also use 1-to-1 NAT to solve the problem when you must create a VPN tunnel between two networks that use the same private network address. When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT. Then, you can create the VPN tunnel and not change the IP addresses of one side of the tunnel. 1-to-1 NAT for

a VPN tunnel is configured when you configure the VPN tunnel and not in the **Network > NAT** dialog box.

Configuring firewall 1-to-1 NAT

1 From Policy Manager, click **Network > NAT**. Click the **1-to-1 NAT** tab.

2 Click **Add**.
The 1-1 Mapping dialog box appears.


Add 1-to-1 Mapping
Type
Map Type: IP Range
Maps one IP address range to another IP address range of the same size
Configuration
Select the interface and the number of hosts to be translated. Then, specify the base for the exposed NAT range and the real IP address range.
Interface: External
No of Hosts to NAT: 5
NAT Base: 50. 1 . 1 .1
Real Base: 10. 1 . 1 .1
OK
Cancel

3 In the **Map Type** drop-down list, select **Single IP**, **IP range**, or **IP subnet** if you want to map to one host, a range of hosts, or a subnet.

4 In the **NAT base** text box, type the address for the NAT range to see externally.

5 Complete all the information. Click **OK**.

6 Repeat steps 2 – 4 for each 1-to-1 NAT entry. When you are done, click **OK** to close the **NAT Setup** dialog box. Save the changes to the Firebox.

After you configure a global 1-to-1 NAT rule, you must configure the NAT base IP addresses in the appropriate policies. In the example given above, we must configure our SMTP policy to allow SMTP traffic from Any to 50.1.1.1-50.1.1.5.

Configuring policy-based 1-to-1 NAT

With this type of NAT, the Firebox uses the private and public IP ranges that you set when you configured global 1-to-1 NAT, but the rules are applied to an individual policy. 1-to-1 NAT is enabled in the default configuration of each policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, the 1-to-1 NAT gets precedence. 1-to-1 NAT will not disable dynamic NAT for the policy.

Disabling policy-based 1-to-1 NAT

1 From Policy Manager, right-click a policy and select **Edit**.

2 The **Edit Policy Properties** window appears.

3 Click the **Advanced** tab.

4 Clear the **1-to-1 NAT** check box to turn NAT off for the traffic this policy controls.

5 Click **OK**. Save the change to the Firebox.

Configuring policy-based dynamic NAT

With this type of NAT, the Firebox maps private IP addresses to public IP addresses. Dynamic NAT is enabled in the default configuration of each policy. Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the Firebox. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, the 1-to-1 NAT gets precedence. 1-to-1 NAT will not disable dynamic NAT for the policy.

You also have the option to set a dynamic NAT source IP address for any policy that uses dynamic NAT. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. You would most often do this to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the Firebox's external interface is not the same as your MX record IP address.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

Note

If you use multi-WAN, you cannot use the **Set Source IP** option. Use this option only when your Firebox uses a single external interface.

Disabling policy-based dynamic NAT

1 From Policy Manager, right-click a policy and select **Edit**.

2 The **Edit Policy Properties** window appears.

3 Click the **Advanced** tab.

4 Clear the **Dynamic NAT** check box to turn dynamic NAT off for the traffic this policy controls.

Configuring Static NAT for a Policy

Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall. If a software application uses more than one port and the ports are selected dynamically, you must use 1-to-1 NAT or check if there is a proxy on the Firebox® to manage this kind of traffic.

When you use static NAT, you use an external IP address of your Firebox instead of the IP address of a public server. You could do this because you want to, or because your public server does not have a public IP address. For example, you can put your SMTP e-mail server behind the Firebox with a private IP address and configure static NAT in your SMTP policy. The Firebox receives connections on port 25 and makes sure that any SMTP traffic is sent to the real SMTP server behind the Firebox.

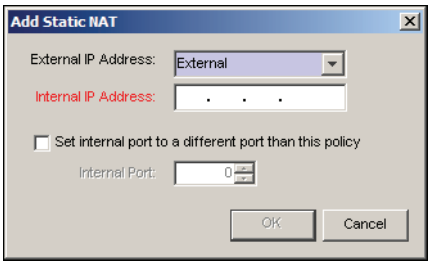
Because of how static NAT works, it is available only for policies that use a specified TCP or UDP port. A policy that has another protocol cannot use incoming static NAT. If you have a policy that uses a protocol other than TCP or UDP, the **NAT** button in the **Properties** dialog box of that policy is disabled. You also cannot use static NAT with the Any policy.

1 Double-click a policy icon in the Policies Arena.

2 From the **Connections are** drop-down list, select **Allowed**.
To use static NAT, the policy must let incoming traffic through.

3 Below the **To** list, click **Add**.
The Add Address dialog box appears.

4 Click **NAT**.
The Add Static NAT dialog box appears.



5 From the **External IP Address** drop-down list, select the public IP address to use for this service.

6 Type the internal IP address.
The internal IP address is the destination on the trusted or optional network.

7 If necessary, select the **Set internal port to different port than this policy** check box. This enables port address translation (PAT).
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the different port number or use the arrow buttons in the Internal Port box.

8 Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.

9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Properties** dialog box of the service.

CHAPTER 10

Implementing Authentication

User authentication allows user names to be associated with connections through the Firebox. When you use user authentication, a Firebox administrator can see user names and IP addresses when they monitor connections through the Firebox. Without authentication, you see only the IP address of each connection. With authentication, a user can log in to the network from any computer, but see only the information for which they are authorized. All the connections that the user starts from that IP address also transmit the session name while the user is authenticated.

The Firebox allows you to create policies that include groups and user names. As a result, the policy is applied to any computer a person uses to log in. Monitor by user name:

- If you use Dynamic Host Configuration Protocol (DHCP). DHCP can cause the IP address of a computer to change.
- If many different users can use the same IP address in a day, such as in a university or computer lab environment.

In these cases, authentication gives you more information about the employee actions.

How User Authentication Works

An HTTPS server operates on the Firebox® to accept authentication requests. To authenticate, a user must connect to the authentication web page on the Firebox. The address is:

https://*IP address of a Firebox interface*:4100/
or
https://*Host name of the Firebox*:4100

An authentication web form appears. The user must type their user name and password. The Firebox sends the name and password to the authentication server using PAP (Password Authentication Protocol). When the user is authenticated, the user is then allowed to use the approved network resources. The user is authenticated for some time after they close their last authenticated connection. This authentication time-out is set by the Firebox administrator in **Policy Manager > Setup > Global Settings**.

To close an authenticated session before the authentication time-out occurs, a user can click **Logout** on the Authentication web page. If the page is closed, the user must open it again to disconnect. To pre-

vent a user from authenticating, the administrator must disable that user's account on the authentication server.

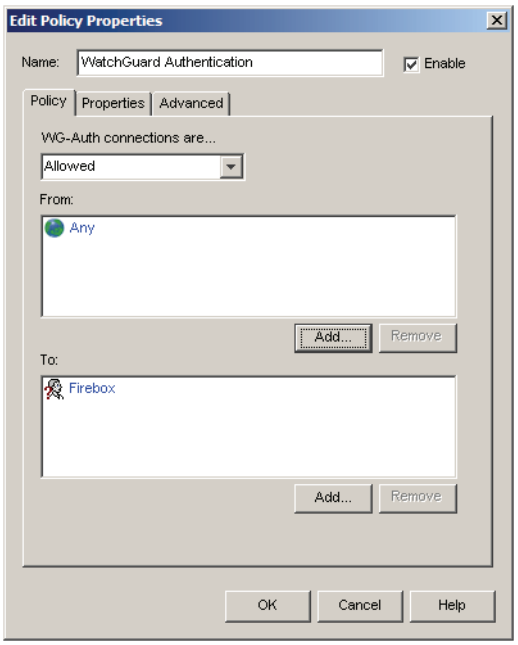
Using authentication from the external network

The primary function of the authentication tool is to authenticate outgoing traffic. You can also use it to restrict incoming network traffic. When you have an account on the Firebox, you can always use external authentication. For example, you can type this address in your browser at home:
https://IP address of Firebox external interface:4100/

After you authenticate, you can use the policies that are configured for you on the Firebox.

Use this procedure to let a remote user authenticate from the external network. This lets the person use resources through the Firebox.

1. From Policy Manager, double-click the **WatchGuard Authentication** policy icon. This policy appears after you add a user or group to a policy configuration.
   You see a warning to be careful when you edit an automatically configured policy.
2. Click the **Policy** tab.
3. From the **WG-Auth connections are** drop-down list, select **Allowed**.
4. Below the **From** box, click **Add**. Select **Any** from the list and click **Add**. Click **OK**.
5. Below the **To** box, click **Add**. Select **Firebox** from the list and click **Add**. Click **OK**.



Using authentication through a gateway Firebox to another Firebox

To send an authentication request through a gateway Firebox to a different Firebox, you must add a policy that allows the authentication traffic on the gateway Firebox. On the gateway Firebox, use Policy Manager to add the WatchGuard Authentication policy. This policy controls traffic on TCP port 4100. Configure the policy to allow traffic to the IP address of the destination Firebox.

Authentication server types

With Fireware®, there are five authentication methods:

- Firebox
- RADIUS
- SecurID
- LDAP
- Active Directory

You can configure one or more authentication server types for a Firebox. Authentication to different server types is almost the same for the user. For the Firebox administrator, the difference is that the user database can be on the Firebox or on a dedicated authentication server.

When you use an authentication server, you configure it with the instructions from its manufacturer. You install the server with access to the Firebox and put it behind the Firebox for security.

Using a backup authentication server

You can configure a backup authentication server with all types of third-party authentication. If the Firebox cannot connect to the primary authentication server (after three attempts), it connects to the backup authentication server. If the Firebox cannot connect to the backup authentication server, it waits ten minutes, and then tries to connect to the primary authentication server again. This cycle continues until the Firebox connects with an authentication server.

Configuring the Firebox as an Authentication Server

If you do not use a third-party authentication server, you can use the Firebox® as an authentication server. This procedure divides your company into groups and users for authentication. The group to which you assign a person is controlled by the tasks they do and information they use. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new employee group, with controlled access to the Internet.

In a group, you set the authentication procedure for the users, the system type, and the information to which they have access. A user can be a network or a computer. If your company changes, you can add or remove users or systems from your groups.

Use Policy Manager to:

- Add, change, or delete the groups in the configuration
- Add or change the users in a group

About Firebox authentication

You can configure the Firebox to authenticate users for three different types of authentication:

- Firewall authentication
- PPTP connections
- MUVPN connections

When the authentication is successful, the Firebox makes a mapping between these items:

- User name
- Firebox User group (or groups) of which the user is a member
- IP address on the user's computer when the user authenticates

- Virtual IP address on the user's computer if the user is connected with RUVPN.

Firewall authentication

To create a Firebox user account, from Policy Manager, select **Setup > Authentication Servers**. After you create the user account, you can make a Firebox group and put the user in that Firebox User group.

Next, create a policy that allows traffic only to or from a list of Firebox user names or a list of Firebox groups. This policy is applied only if a packet comes from or goes to the authenticated user's IP address.

A user authenticates with an HTTPS connection to the Firebox over port 4100 by typing:
https://*IP address of a Firebox interface*:4100/
If the user name and password are valid, the user is authenticated.

When a user is authenticated, the user credentials and IP address of their computer are both used to find if a policy applies to the traffic starting from or going to that user's computer.

PPTP connections

To configure the Firebox to host PPTP VPN sessions, select **VPN > Remote Users** and click the **PPTP** tab. If you do not select the check box **Use RADIUS Authentication to authenticate remote users**, then the Firebox authenticates the PPTP session. The Firebox checks to see if the user name and password the user enters into the VPN connection box matches the user name and password in the Firebox User database. If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.

Next, create a policy that allows traffic only from or to a list of Firebox user names, or a list of Firebox groups. The Firebox does not look at this policy unless traffic comes from or goes to the authenticated user's virtual IP address.

The user makes the PPTP connection using the PPTP feature included in their computer operating system. Because the Firebox allows the PPTP connection from any Firebox user that gives the correct credentials, it is important that you make a policy for PPTP sessions that includes only users you want to allow to send traffic over the PPTP session. Or, put these users into a Firebox User group and make a policy that allows traffic only from this group. The Firebox has a pre-configured group for this called "PPTP-Users".

MUVPN connections

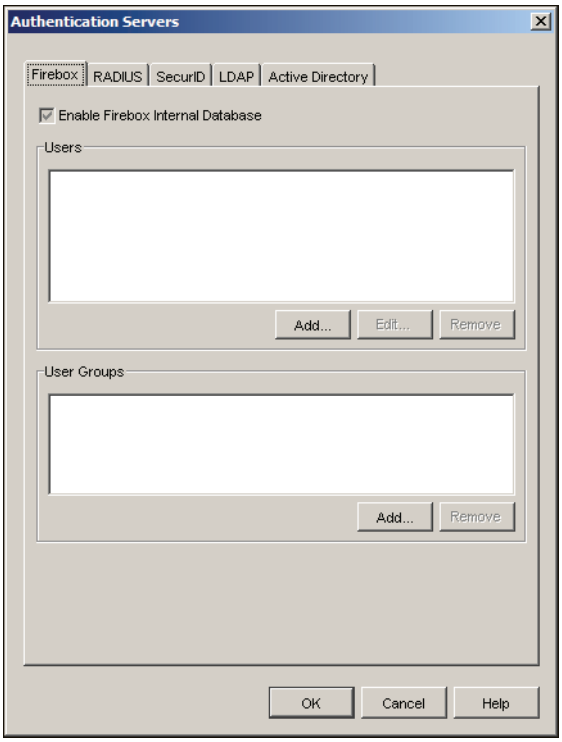
You can configure the Firebox to host Mobile User VPN (MUVPN) IPSec sessions. To do this, select **VPN > Remote Users** and click the **Mobile User VPN** tab. You make the MUVPN group using the Add Mobile User VPN wizard. When the wizard is finished, Policy Manager does two things:

- Makes a client configuration profile (called a .wgx file) and puts it on the management station computer that created the MUVPN account. The user must have this .wgx file to configure the MUVPN client computer.
- Automatically adds an "Any" policy to the **Mobile User VPN** tab that allows traffic to pass to and from the authenticated MUVPN user.

When the user's computer is correctly configured, the user makes the MUVPN connection. If the user name and password the user enters into the MUVPN authentication dialog box match an entry in the Firebox User database, and if the user is in the MUVPN group you create, the MUVPN session is authenticated. Policy Manager automatically makes a policy that allows any traffic from the authenticated user. To restrict the ports the MUVPN client can access, delete the Any policy and add policies for those ports to the **Mobile User VPN** tab. To learn how to add policies, see "Adding Policies" on page 146.

Setting up the Firebox as an authentication server

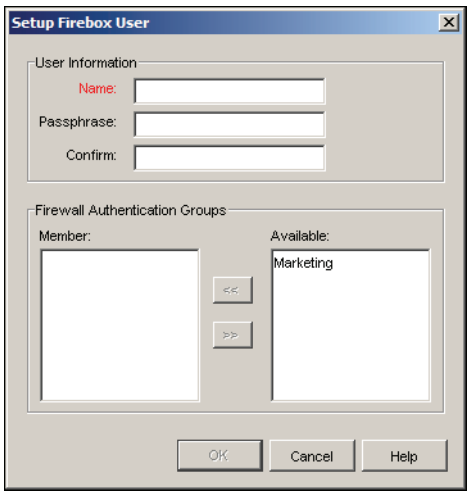
1 From Policy Manager, select **Setup > Authentication Servers**.
The Authentication Servers dialog box appears. The default configuration enables the Firebox authentication server.



2 To add a new user group, click **Add** below the **User Groups** list.
The Add Firebox Group dialog box appears.

3 Type the group name that you want. Click **OK**.

4 To add a new user, click **Add** below the **Users** list.
The Setup Firebox User dialog box appears.



5 Type the name and the passphrase you want the person to use to authenticate to the Firebox.
When this passphrase is set, you cannot see the passphrase in simple text again. If you lose the passphrase, you must set a new passphrase.

6 To add the user to a group, select the group name in the **Available** list. Click the double arrow that points left to move the name to the **Member** list.
You can also double-click the group name.

7 Add the user to the PPTP-Users group if you want to use the PPTP-Users group in a service.

8 After you add the user to selected groups, click **OK**.
The user is added to the user list. You can then add more users.

9 To close the **Setup Firebox User** dialog box, click **OK**.
The Firebox Users tab appears with a list of the new users.

10 After you add all necessary users and groups, click **OK**. At this time, you can use the users and groups to configure policies and authentication.

Using a local user account for Firewall user, PPTP, and MUVPN authentication

Any user can authenticate as a Firewall user, PPTP user, or MUVPN user, and open a PPTP or MUVPN tunnel if PPTP or MUVPN is enabled on the appliance. However, after an authentication or tunnel has been successfully established, users can send traffic through the VPN tunnel only if the traffic is allowed by a policy on the Firebox. For example, an MUVPN-only user can send traffic through an MUVPN tunnel, but not a PPTP tunnel even though the user can authenticate and bring up a PPTP tunnel.

1 Enable and configure firewall user authentication, MUVPN, and PPTP to use local accounts.

2 Create appropriate policies for these authentication types.

3 Associate an user account to each authentication group (FW-Users, PPTP-Users, MUVPN-Users). Also create an account that does not belong to any group.

4 Deploy the configuration to the Firebox.

5 Use a web browser, PPTP client, and MUVPN client to authenticate to the Firebox with each of these user accounts.

Configuring RADIUS Server Authentication

Remote Authentication Dial-In User Service (RADIUS) authenticates the local users and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

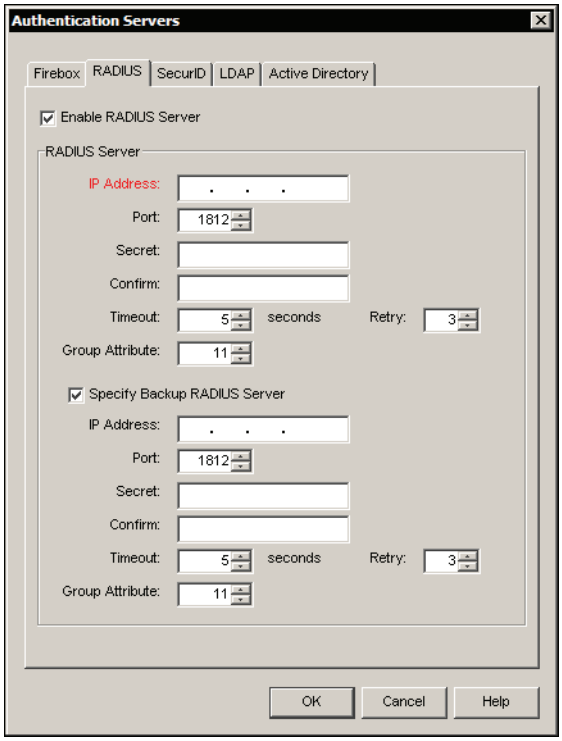
The authentication messages to and from the RADIUS server always use an authentication key. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, hackers cannot get to the authentication messages. Note that RADIUS sends a key, and not a password, during authentication. For web and MUVPN authentication, RADIUS supports only PAP (not CHAP) authentication. For authentication with PPTP, RADIUS supports only MSCHAPv2.

To use RADIUS server authentication with the Firebox®, you must:

- Add the IP address of the Firebox to the RADIUS server, as described in the RADIUS documentation.
- Enable and specify the RADIUS server in your Firebox configuration.
- Add RADIUS user names or group names into the policies in Policy Manager.

To enable RADIUS Server Authentication:

1 From Policy Manager, select **Setup > Authentication Servers**. Click the **RADIUS Server** tab.
The RADIUS configuration appears.



2 In the **IP Address** box, type the IP address of the RADIUS server.

3 In the **Port** box, make sure that the port number RADIUS uses for authentication appears.
The default port number is 1812. Older RADIUS servers might use port 1645.

4 In the **Secret** box, type the shared secret between the Firebox and the RADIUS server.
The shared secret is a password that is case-sensitive, and it must be the same on the Firebox and the RADIUS server.

5 To set the time-out value, use the **Timeout** value control to set the value you want.
This sets how long the Firebox waits for a response from the authentication server before it tries to connect again.

6 To set how many connection attempts the Firebox makes, use the **Retry** value control to set the number you want.
This is the number of times the Firebox tries to connect to the authentication server (using the time-out specified above) before it reports a failed connection for one authentication attempt.

7 To set the group attribute, use the **Group Attribute** value control to set the attribute you want.
The group attribute value is used to set which attribute carries the User Group information. When the RADIUS server sends a message to the Firebox that a user is authenticated, it also sends a User Group string; for example, "engineerGroup" or "financeGroup". This information is then used for access control.

8 To add a backup RADIUS server, select the **Specify Backup RADIUS Server** check box. If you select the check box, type the IP address and the port of the backup RADIUS server. The shared secret must be the same on the primary and backup RADIUS server.

9 Click **OK**.

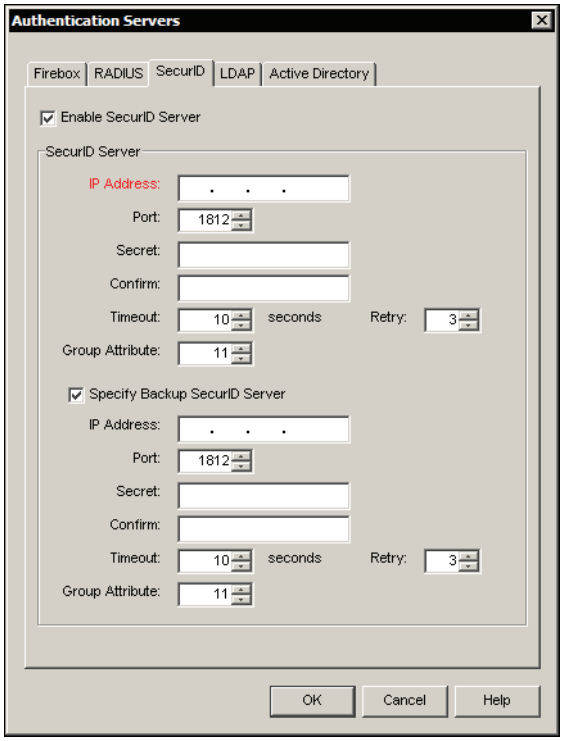
Configuring SecurID Authentication

To use SecurID authentication, you must configure RADIUS and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN (personal identification number). Refer to the SecurID instructions for more information.

Note

Do not use Steel Belted RADIUS with SecurID. Use the RADIUS software application with RSA SecurID software.

1 From Policy Manager, select **Setup > Authentication Servers**. Click the **SecurID Server** tab.



2 In the **IP Address** box, type the IP address of the SecurID server.

3 In the **Port** box, use the value control to select the port number to use for SecurID authentication.
The default number is 1812.

4 In the **Secret** box, type the shared secret between the Firebox® and SecurID server.
The shared secret is a case-sensitive password and must be the same on the Firebox and SecurID server.

5 In the **Timeout** box, use the value control to select the timeout value you want.
This sets how long the Firebox waits for a response from the authentication server before it tries to connect again.

6 To set how many connection attempts the Firebox makes, use the **Retry** value control.
This is the number of times the Firebox tries to connect to the authentication server (using the time-out specified above) before it reports a failed connection for one authentication attempt.

7 Select the group attribute. We do not recommend that you change this value.
The group attribute value is used to set which attribute carries the User Group information. When the SecurID server sends a message to the Firebox that a user is authenticated, it also sends a User Group string; for example, "engineerGroup" or "financeGroup". This information is then used for access control.

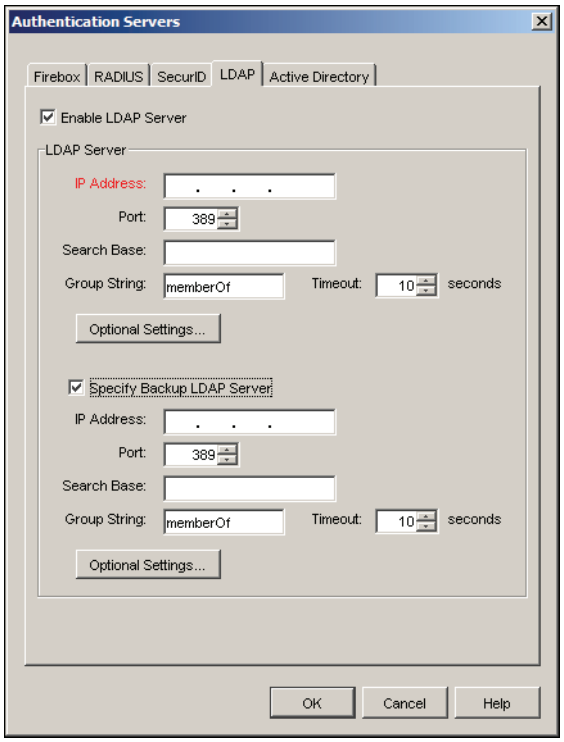
8 Type the IP address and the port of the backup SecurID server. The shared secret must be on the primary and backup SecurID server.

9 Click **OK**.

Configuring LDAP Authentication

You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users to the Firebox®. LDAP is an open-standard protocol for using online directory services, and it operates with Internet transport protocols, such as TCP. You can use LDAP to get access to stand-alone directory servers or X.500 directories.

1 From Policy Manager, select **Setup > Authentication Servers**. Select the **LDAP** tab.



2 Select the **Enable LDAP Server** check box.

3 In the **IP Address** box, type the IP address of the primary LDAP server for the Firebox to contact with authentication requests.
The LDAP server can be located on any Firebox interface or available through a VPN tunnel.

4 From the **Port** drop-down list, select the TCP port number for the Firebox to use to connect to the LDAP server. The default port number is 389.
We do not support SSL binds on port 636.

5 Type the **Search Base**. The standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after the dot.
For example, if your user accounts are in an OU (organizational unit) you refer to as "accounts" and your domain name is kunstlerandsons.com, your search base is:
"ou=accounts,dc=kunstlerandsons,dc=com".
You set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.

6 Type the **Group String**.
The attribute string that is used to hold user group information on the LDAP server. On many LDAP servers, the default group string is "uniqueMember"; on other servers it is "member".

7 If necessary, change the time-out value. This is how long the Firebox waits for a response from the authentication server.

8 Add information for a backup LDAP Server, if you have one.

9 To configure MUVPN users to get configuration information from the LDAP Server, you can change your directory schema and use the settings available through the **Optional Settings** button. You can enter MUVPN client information in the user properties of your LDAP Server, which includes the IP address, subnet mask, or DNS and WINS servers. Then, you can map these fields to the fields that appear in Optional Settings. When the MUVPN user starts a VPN tunnel through the Firebox, the Firebox sets the IP address, subnet mask, or DNS and WINS servers for the user with the information contained in the LDAP user properties.

IP *Attribute String*
Type the name of the LDAP user property field name that contains the assigned IP address.

Netmask Attribute String
Type the name of the LDAP user property field name that contains the assigned subnet mask.

DNS Attribute String
Type the name of the LDAP user property field name that contains the DNS server IP address.

WINS Attribute String
Type the name of the LDAP user property field name that contains the WINS server IP address.

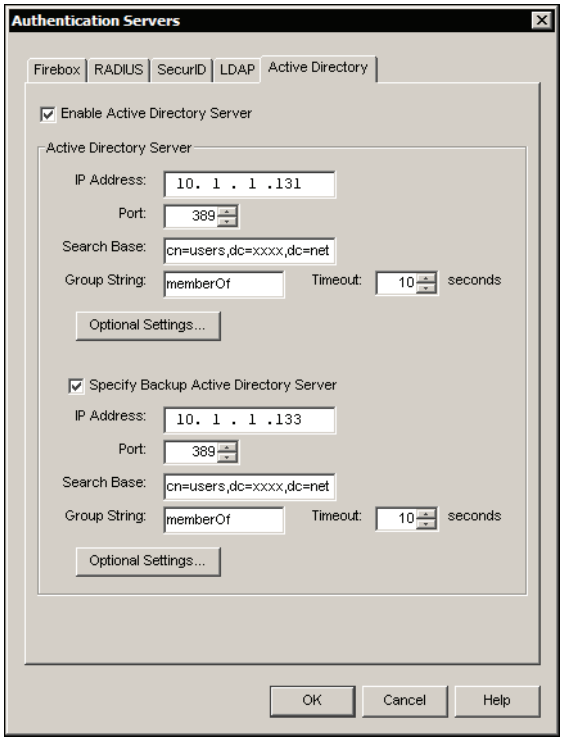
Lease Time Attribute String
Type the name of the LDAP user property field name that contains the total time allowed for the MUVPN connection session.

Idle Timeout Attribute String
Type the name of the LDAP user property field name that contains the assigned idle time-out.

Configuring Active Directory Authentication

You can use an Active Directory authentication server to authenticate your users to the Firebox. You must configure the Firebox® and configure the Active Directory server.

1 From Policy Manager, select **Setup > Authentication Servers**. Select the **Active Directory** tab.



2 Select the **Enable Active Directory Server** check box.

3 Type the IP address of the primary Active Directory server.
The Active Directory server can be located on any Firebox interface or available through a VPN tunnel.

4 Select the TCP port number for the Firebox to use to connect to the Active Directory server. The default port number is 389.
If your Active Directory server is a global catalog server, it can be useful to change the default port. For more information, see https://www.watchguard.com/support/Fireware_Howto/HowTo_UseGlobalCatalogPort.pdf.

5 Type the **Search Base**. The standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after the dot.
For example, if your user accounts are in an OU (organizational unit) you refer to as "accounts" and your domain name is HQ_main.com, your search base is: "ou=accounts,dc=HQ_main,dc=com".
You set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.

6 Type the **Group String**.
This is the attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always "memberOf".

7 If necessary, change the time-out value. This is the time the Firebox waits for a response from the authentication server.

8 Add information for a backup Active Directory server, if you have one.

9 To configure MUVPN users to get configuration information from the Active Directory server, you can change your directory schema and use the settings available through the **Optional Settings**

button. You can enter MUVPN client information in the user properties of your Active Directory Server, which includes the IP address, subnet mask, or DNS and WINS servers. Then, you can map these fields to the fields that appear in Optional Settings. When the MUVPN user starts a VPN tunnel through the Firebox, the Firebox sets the IP address, subnet mask, or DNS and WINS servers for the user with the information that appears in the Active Directory user properties.

IP Attribute String
: Type the name of the Active Directory user property field name that contains the assigned IP address.

Netmask Attribute String
: Type the name of the Active Directory user property field name that contains the assigned subnet mask.

DNS Attribute String
: Type the name of the Active Directory user property field name that contains the DNS server IP address.

WINS Attribute String
: Type the name of the Active Directory user property field name that contains the WINS server IP address.

Lease Time Attribute String
: Type the name of the Active Directory user property field name that contains the assigned lease time.

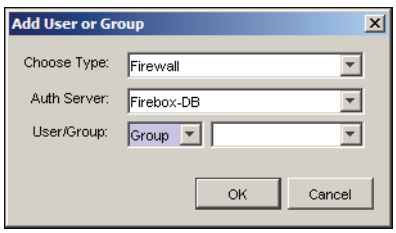
Idle Timeout Attribute String
: Type the name of the Active Directory user property field name that contains the assigned idle time-out.

Configuring a Policy with User Authentication

When you configure the Firebox® to use an authentication server, you can start to use user names when creating policies in Policy Manager. For example, you can put a limit on all policies that connections are allowed only for authenticated users. To do this:

1 Create a group on your third-party authentication server that contains all the user accounts.

2 In Policy Manager, add or start your Outgoing policy. Below the **From** field, click **Add** and then click **Add User**.
The Add User or Group dialog box appears.



3 From the **Choose Type** drop-down list, select firewall, MUVPN, or PPTP authentication.

4 From the **Auth Server** drop-down list, select the type of authentication server to use.

5 From the **User/Group** drop-down list, select **User** or **Group**.

6 Type the user or group name you created on the authentication server. Click **OK**.

7 Configure the **From** fields on all policies in Policy Manager the same way.

8 After you add a user or group to a policy configuration, WatchGuard System Manager automatically adds a WatchGuard Authentication policy to your Firebox configuration. Use this policy to control access to the authentication web page.

CHAPTER 11

Firewall Intrusion Detection and Prevention

WatchGuard® Fireware® and the policies you create in Policy Manager give you strict control over access to your network. A strict access policy helps keep hackers out of your network. But, there are other types of attacks that a strict policy cannot defeat. Careful configuration of the Firebox® default packet handling options can stop attacks such as SYN flood attacks, spoofing attacks, and port or address space probes.

With default packet handling, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If there is a risk, you can configure the Firebox to automatically block against the possible attack. This proactive method of intrusion detection keeps attackers out of your network. You can also purchase an upgrade for your Firebox to use signature-based intrusion prevention. For more information, see the chapter "Signature-Based Intrusion Detection and Prevention" in this manual.

Using Default Packet Handling Options

The firewall examines the source and destination of each packet it receives. It looks at the IP address and the port number. The firewall also monitors the packets to look for patterns that can show that your network is at risk.

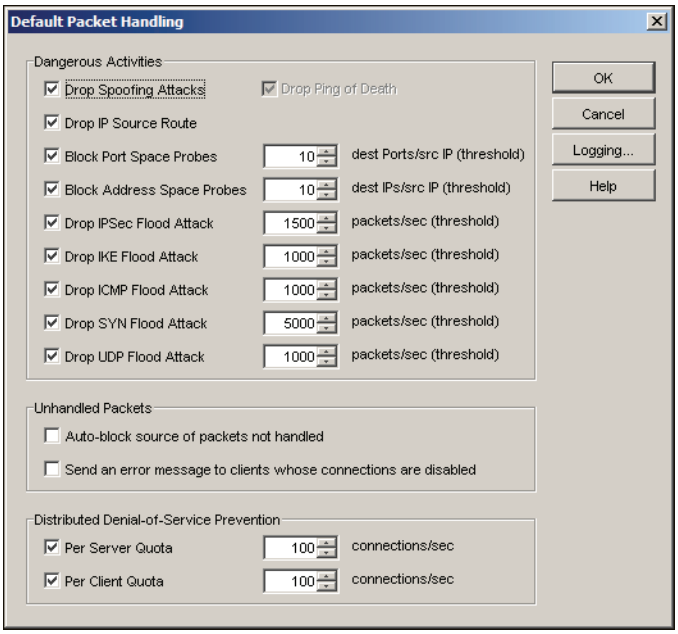
Default packet handling:

- Rejects a packet that can be a security risk, including packets that could be part of a spoofing attack or SYN flood attack
- Can automatically block all traffic to and from a source IP address
- Adds an event to the log file
- Sends an SNMP trap to the SNMP management server
- Sends a notification of possible security risks

You set all default packet handling options with the **Default Packet Handling** dialog box.

1 From Policy Manager, select **Setup > Intrusion Prevention > Default Packet Handling**.
or,
Click the default packet handling icon on the Policy Manager toolbar.
The Default Packet Handling dialog box appears.

2 Select the check box for the traffic patterns you want to prevent, as explained in the sections that follow. The default configuration sends a log message when one of these events occur. To configure an SNMP trap or notification for default packet handling, click **Logging**.



Spoofing attacks

One procedure that attackers use to get access to your network is to make an "electronic false identity." With this "IP spoofing" procedure, the attacker sends a TCP/IP packet that uses a different IP address than the host that first sent it.

With IP spoofing enabled, the Firebox® checks to make sure that the source IP address of a packet is from a network on that interface.

To protect against spoofing attacks, select the **Drop Spoofing Attacks** check box from the **Default Packet Handling** dialog box.

IP source route attacks

Attackers use IP source route attacks to send an IP packet to find the route that the packet uses to go through the network. The attacker can then see the response to the packets and get information about the operating system of the target computer or network.

To protect against IP source route attacks, select the **Drop IP Source Route** check box from the **Default Packet Handling** dialog box.

"Ping of death" attacks

"Ping of death" is a denial of service (DoS) attack. It is caused by an attacker that sends an IP packet that is larger than the 65,535 bytes allowed by the IP protocol. This causes some operating systems to crash or restart.

To protect against ping of death attacks, the **Drop Ping of Death** feature is always enabled. You cannot disable this feature.

Port space and address space attacks

Attackers use probes to find information about networks and their hosts. Port space probes examine a host to find the services that it uses. Address space probes examine a network to see which hosts are on that network.

To protect against port space and address space attacks, select the **Block Port Space Probes** and the **Block Address Space Probes** check boxes from the **Default Packet Handling** dialog box. You then use the arrows to select the maximum allowed number of IP addresses or port probes for each source IP address.

Flood attacks

In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives sufficient ICMP ping commands that it uses all of its resources to send reply commands. The Firebox can protect against these types of flood attacks:

- IPSec flood attacks
- IKE flood attacks
- ICMP flood attacks
- SYN flood attacks
- UDP flood attacks

Flood attacks are also known as Denial of Service (DoS) attacks. You can use the **Default Packet Handling** dialog box to configure the Firebox to protect against these attacks. Select the check boxes for the flood attacks you want to prevent. Use the arrows to select the maximum allowed number of packets each second.

About the SYN flood attack setting

For SYN flood attacks, you set the threshold for the Firebox to report that a SYN flood attack may be taking place. But, no packets are dropped if only that number of packets is received. At twice the threshold, all SYN packets are dropped. At any level between the threshold you define and twice that level, if a packet's src_IP, dst_IP, and total_length are the same as the previous packet received, then it will always be dropped; otherwise 25 percent of the new packets received are dropped.

For example, suppose you define the threshold at 18 packets per second. When you receive that amount, the Firebox warns you that a SYN flood attack may be taking place but it drops no packets. If you receive 20 packets per second, the FB drops 25% of the packets (5 packets). If you receive 36 or more, the last 18 or more packets are dropped.

Unhandled packets

An “unhandled” packet is a packet that does not match any rule created in Policy Manager. The Firebox always denies the packet, but you can also select to always automatically block the source. This adds the IP address that sent the packet to the temporary Blocked Sites list. You can also send a TCP reset or ICMP error back to the client when an unhandled packet is received by the Firebox.

Distributed denial of service attacks

Distributed Denial of Service (DDoS) attacks are almost the same as flood attacks. In a DDoS, the ICMP ping commands come from many computers. You can use the **Default Packet Handling** dialog box to

configure the Firebox to protect against DDoS attacks. Use the arrow keys to set the maximum allowed number of connections that your servers and clients can receive each second.

Setting Blocked Sites

The Blocked Sites feature helps prevent network traffic from systems you know or think are dangerous or a security risk. After you find the source of suspicious traffic, you can block all the connections with that IP address. You can also configure the Firebox to send a log message each time the source tries to connect to your network. From the log file, you can see the services that they use to attack.

A blocked site is an IP address that cannot make a connection through the Firebox. If a packet comes from a system that is blocked, it does not get through the Firebox®.

There are two different types of blocked IP addresses:

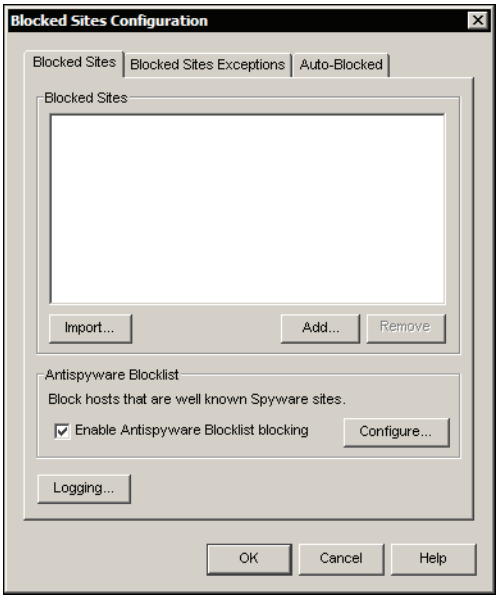
- Permanently blocked sites — on a list in the configuration file that you set manually. This is known as the Blocked Sites list.
- Auto-blocked sites — IP addresses that the Firebox adds or removes on a temporary blocked site list. The Firebox uses the packet handling rules that are specified for each service. For example, you configure the Firebox to block the IP addresses that try to connect to a blocked port. These addresses are then blocked for a specified time. This is known as the Temporary Blocked Sites list.

You can use a list of temporarily blocked sites with log messages to help you make a decision about which IP addresses to block permanently.

Blocking a site permanently

You use Policy Manager to permanently block a host that you know is a security risk. For example, a university computer that hackers use frequently is a good host to block.

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Sites**.
The Blocked Sites Configuration dialog box appears.



2 Click **Add**.
The Add Site dialog box appears.

3 Use the **Choose Type** drop-down list to select a member type. The selections are **Host IP**, **Network IP**, or **Host Range**.

4 Type the member value.
The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the tab or the arrow key.

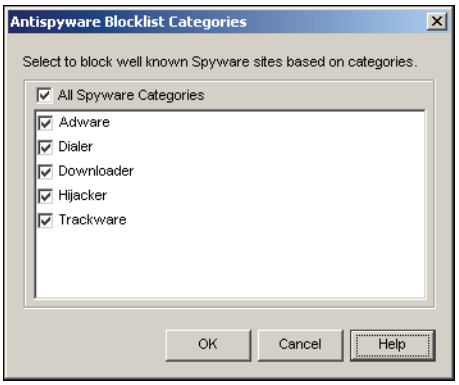
5 Select **OK**.
The new site appears in the Blocked Sites list.

Blocking spyware sites

You can block spyware by configuring categories of spyware sites to block.

1 From the **Blocked Sites** dialog box, select the **Enable Antispyware Blocklist blocking** check box.

2 By default, the Firebox blocks all categories of spyware when you select the check box in the previous step. To choose which categories of spyware you want to block, click **Configure**.
The Antispyware Blocklist Categories dialog box appears.



3 Select or clear the following check boxes to enable or disable antispyware blocking for these categories. To enable or disable all categories, select or clear the **All Spyware Categories** check box:

Adware
A software application in which advertising banners are shown while the program is in operation. It sometimes includes code that records a user's personal information and sends it to third parties, without the user's authorization or knowledge.

Dialer
A software application that can hijack a user's modem and dial toll numbers that get access to inappropriate web sites.

Downloader
A program that gets and installs other files. Most are configured to get files from a designated web or FTP site.

Hijacker
A type of malware program that changes your computer's browser settings and redirects you to web sites that you did not plan to browse to.

Trackware
Any software that uses a computer's Internet connection to send personal information without the user's permission.

Using an external list of blocked sites

You can make a list of blocked sites in an external file. This file must be a .txt file. To add an external file to your Blocked Sites list:

1 In the **Blocked Sites Configuration** dialog box, select **Import**.

2 Find the file. Double-click it, or select it and select **Open**.
The sites in the file appear in the Blocked Sites list.

Creating exceptions to the Blocked Sites list

A host that is a blocked sites exception does not appear in the Blocked Sites list. The automatic rules do not apply for this host.

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Sites**.

2 Click the **Blocked Sites Exceptions** tab. Click **Add**.

3 Use the **Choose Type** drop-down list to select a member type. The selections are **Host IP**, **Network IP**, or **Host Range**.

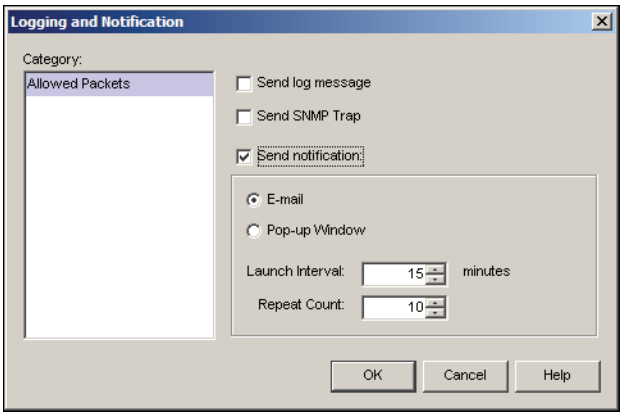
4 Type the member value.
The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the TAB or the arrow key.

5 Select **OK**.

Setting logging and notification parameters

You can configure the Firebox to make a log entry when a host tries to use a blocked site. You can also set up notification for when a host tries to get access to a blocked site.

1 From the **Blocked Sites** dialog box, select **Logging**.
The Logging and Notification dialog box appears.



2 Set the parameters and notification to comply with your security policy:

Enter it in the log

When you enable this check box, the Firebox sends a log message when a packet is denied because of your blocked port configuration. The default configuration of all services is for the Firebox to send a log message when it denies a packet.

Send SNMP trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The SNMP trap makes sure that traffic matches allowed values. An example of criteria it examines is a threshold limit.

Send notification

When you enable this check box, the Firebox sends a notification when a packet is denied because of your blocked port configuration. You can configure the Firebox to do one of these actions:

- **E-mail** The Firebox sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Firebox makes a dialog box appear on the management station when the event occurs.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, as follows:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log entry about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are configured as:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 a.m. and continues each minute. This starts the logging and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

Blocking sites temporarily with policy settings

You can use the policy configuration to block sites that try to use a denied service:

1 From Policy Manager, double-click the policy icon.
The Properties dialog box appears.

2 On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied**.

3 On the **Properties** tab, select the check box **Automatically block sites that attempt to connect**.
The IP address from the denied packets are added to the temporary Blocked Sites list for 20 minutes (by default).

Blocking Ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. When you block a port, you override all the service configurations.

You can block a port because:

- Blocking ports protects your most sensitive services. The feature helps protect you from errors in your Firebox® configuration.
- Probes against sensitive services can make independent log entries.

With the default configuration, the Firebox blocks some destination ports. This gives a basic configuration that you usually do not have to change. It blocks TCP and UDP packets for these ports:

X Window System (ports 6000-6005)
: The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

X Font Server (port 7100)
: Many versions of X-Windows operate X Font Servers. The X Font Servers operate as the superuser on some hosts.

NFS (port 2049)
: NFS (Network File System) is a frequently used TCP/IP service where many users use the same files on a network. But, the new versions have important authentication and security problems. To supply NFS on the Internet can be very dangerous.

Note

The portmapper frequently uses the port 2049 for NFS. If you use NFS, make sure that NFS uses the port 2049 on all your systems.

rlogin, rsh, rcp (ports 513, 514)
: These services give remote access to other computers. They are a security risk and many attackers probe for these services.

RPC portmapper (port 111)
: The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are easy to attack through the Internet.

port 8000
: Many vendors use this port, and there are many security problems related to it.

port 1
: The TCPmux service uses Port 1, but not frequently. You can block it to make it more difficult for the tools that examine ports.

port 0
: This port is always blocked by the Firebox. You cannot add this port to the Blocked Ports list. You cannot allow traffic on port 0 through the Firebox.

Note

If you must allow traffic through for the types of software applications that use recommended blocked ports, we recommend that you allow the traffic only through an IPSec VPN tunnel or get access to the port using ssh for more security.

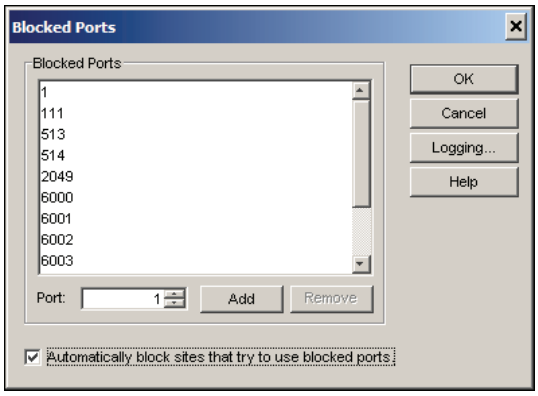
Avoiding problems with blocked ports

You can have a problem because of blocked ports. You must be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.

Blocking a port permanently

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Ports**.
The Blocked Ports dialog box appears.

2 Type the port number. Click **Add**.
The new port number appears in the Blocked Ports list.



Automatically blocking IP addresses that try to use blocked ports

You can configure the Firebox to automatically block an external host that tries to get access to a blocked port. In the **Blocked Ports** dialog box, select the **Automatically block sites that try to use blocked ports** check box.

Setting logging and notification for blocked ports

You can configure the Firebox to make a log entry when a host tries to use a blocked port. You can also set up notification or set the Firebox to send an SNMP trap to an SNMP management server when a host tries to get access to a blocked port.

To set logging and notification parameters for blocked ports, use the same procedure as the one for blocked sites, as described in “Setting logging and notification parameters” on page 140.

CHAPTER 12

Configuring Policies

In Policy Manager, there are two categories of policies: packet filters and proxies.

A *packet filter* examines each packet's IP header and is the most basic feature of a firewall. It controls the network traffic into and out of your Firebox®. If the packet header information is legitimate, then the Firebox allows the packet. If the packet header information is not legitimate, the Firebox drops the packet. It can also record a log message or send an error message to the source.

A *proxy* uses the same procedure to examine the header information as a packet filter, but it also examines the content. If the content does not match the criteria you set, it denies the packet. A proxy operates at the application layer, while a packet filter operates at the network and transport protocol layers. When you activate a proxy, the Firebox:

- Removes all the network data
- Examines the contents for RFC compliance and content type
- Adds the network data again
- Sends the packet to its destination

A proxy uses more resources and bandwidth than a packet filter. But, a proxy looks for dangerous content that a packet filter cannot find.

In this guide, we refer to packet filters and proxies together as policies. Unless we tell you differently, the procedures refer to both proxies and packet filters.

Policy Manager shows each packet filter and proxy as an icon. The traffic is allowed or denied, and you can configure the source and destination. You also set rules for logging and notification and configure the ports, protocols, and other parameters of the packet filter or proxy.

WatchGuard® Fireware® includes many pre-configured packet filters and proxies. For example, if you want a packet filter for all Telnet traffic, you add a Telnet policy. You can also make a custom packet filter for which you set the ports, protocols, and other parameters.

Creating Policies for your Network

The security policy of your organization is a set of rules that define how you protect your computer network and the information that goes through it. The Firebox® denies all packets that are not specially approved. This security policy helps to protect your network from:

- Attacks that use new or different IP protocols
- Unknown applications

When you configure the Firebox with the Quick Setup Wizard, you set only the basic policies (DNS client, FTP, and TCP outgoing proxy) and interface IP addresses. If you have more software applications and network traffic for the Firebox to examine, you must:

- Configure the policies on the Firebox to let necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

We recommend that you set limits on outgoing access when you configure your Firebox.

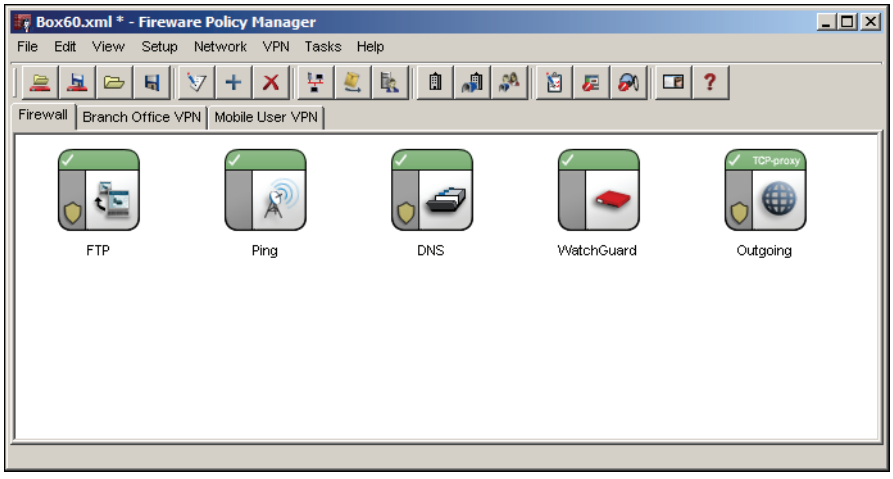
Adding Policies

You add policies with Policy Manager. Policy Manager shows icons or a list to identify the policies that you configure on the Firebox®. For each policy you can:

- Set allowed traffic sources and destinations
- Make filter rules and policies
- Enable or disable the policy
- Configure properties such as QoS, NAT, schedules, and logging

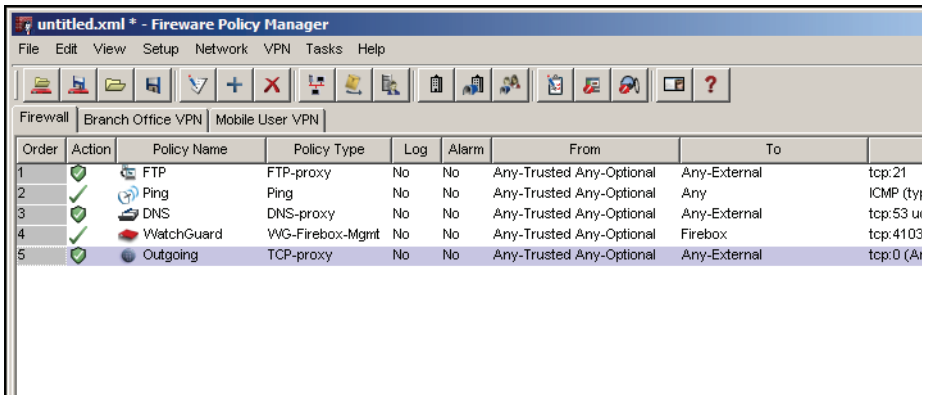
Changing the Policy Manager View

Policy Manager has two views: Large Icons and Details. The Large Icons view shows each policy as an icon. To change to the Large Icons view, select **Large Icons** from the **View** menu.



Large Icons View

To change to the Details view, select **Details** from the **View** menu. In the Details view, each policy is a row. You can see configuration information, including source and destination, and logging and notification parameters.


untitled.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Firewall
Branch Office VPN
Mobile User VPN
Order
Action
Policy Name
Policy Type
Log
Alarm
From
To
1 FTP FTP-proxy No No Any-Trusted Any-Optional Any-External tcp:21
2 Ping Ping No No Any-Trusted Any-Optional Any ICMP (ty
3 DNS DNS-proxy No No Any-Trusted Any-Optional Any-External tcp:53
4 WatchGuard WG-Firebox-Mgmt No No Any-Trusted Any-Optional Firebox tcp:4103
5 Outgoing TCP-proxy No No Any-Trusted Any-Optional Any-External tcp:0

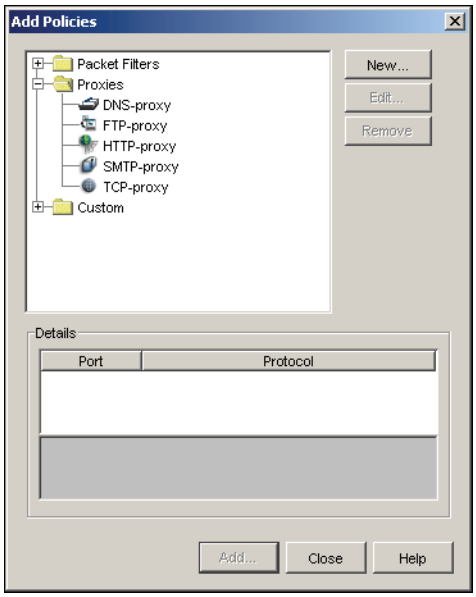
Details View

Adding a policy

You use Policy Manager to add a packet filter or proxy to your configuration. To add a policy:

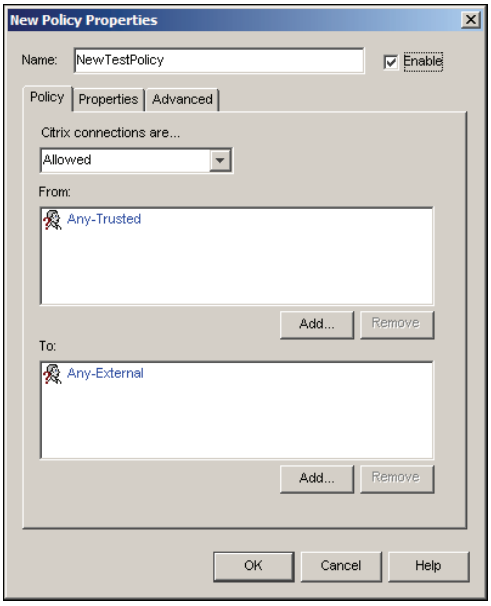
1 In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Add Policies dialog box appears.

2 Click the plus (+) sign on the left side of the folder to expand the **Packet Filters** or **Proxies** folders.
A list of packet filters or proxies appears.



3 Click the name of the policy to add.
When you select a policy, the policy icon appears in the area below the New, Edit, and Remove buttons. Also, the Details box shows the basic information about the policy.

4 Click **Add**.
The New Policy Properties dialog box appears.



5 You can change the name of the policy here. This information appears in the Policy Manager Details view. To change the name, type a new name in the **Name** text box.

6 Click **OK** to close the **Properties** dialog box.
You can add more than one policy while the Policies dialog box is open.

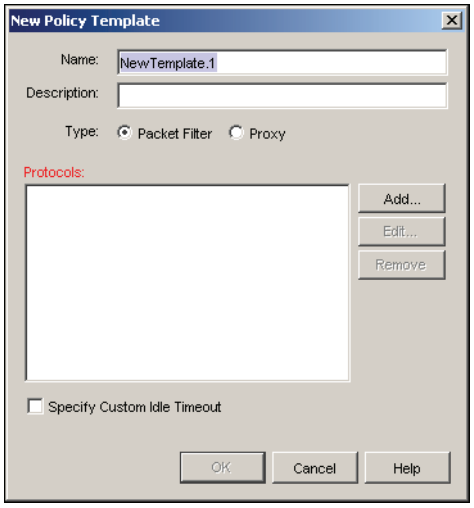
7 Click **Close**.
The new policy appears in Policy Manager. You can now set policy properties, as shown in "Configuring Policy Properties" on page 150.

Making a custom policy template

Policy Manager includes many packet filter policy templates. You can also make a custom policy template. A template includes ports and protocols that are unique to one type of network traffic. It could be necessary to make a custom policy template if you add a new software application behind your firewall.

1 In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Add Policies dialog box appears.

2 Click **New**.
The New Policy Template dialog box appears.



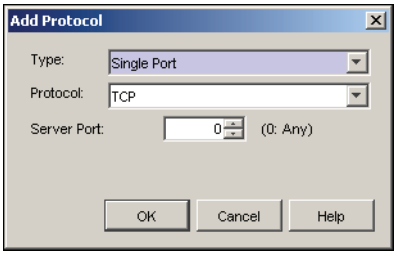
3 In the **Name** text box, type the name of the policy template.
This name must not be the same as any name in the list in the Add Policy dialog box. The name appears in Policy Manager as the policy type. It helps you to find the policy when you want to change or remove it.

4 In the **Description** text box, type a description of the policy.
This appears in the Details section when you click the policy name in the list of User Filters.

5 Select the type of policy: **Packet Filter** or **Proxy**.
The Proxy option gives these options:

- DNS
- FTP
- HTTP
- TCP
- SMTP

6 To add protocols for this policy, click **Add**.
The Add Protocol dialog box appears.



7 From the **Type** drop-down list, select **Single Port** or **Port Range**.

8 From the **Protocol** drop-down list, select the protocol for this new policy. For more information about network protocols, see the *Reference Guide* or online help system. When you select **Single Port**, you can select:

- TCP
- UDP
- GRE
- AH

- ESP
- ICMP
- IGMP
- OSPF
- IP
- Any

When you select **Port Range**, you can select **TCP** or **UDP**.

9 From the **Server Port** drop-down list, select the port for this new policy. If you selected **Port Range**, select a starting server port and an ending server port.

10 Click **OK**.
Policy Manager adds the values to the New Policy Template dialog box. Make sure that the name, information, and configuration of this policy are correct. If necessary, click Add to configure more ports for this policy. Do the Add Port procedure again until you configure all ports for the policy.

11 Click **OK**.
The Add Policy dialog box appears with the new policy in the Custom folder.

Adding more than one policy of the same type

If your security policy lets you, you can add the same policy more than one time. For example, you can set a limit on web access for most users, while you give full web access to your management. To do this, you make two different policies with different properties for outgoing traffic:

1 Add the first policy.

2 Change the name of the policy to give the function in your security policy and add the related information.
In this example, you can name the first policy "restricted_web_access."

3 Click **OK.** The **Properties** dialog box of the policy appears. Set the properties as shown in "Configuring Policy Properties" on page 150.

4 Add the second policy.

5 Click **OK.** The **Properties** dialog box of the policy appears. Set the properties.

Deleting a policy

As your security policy changes, you sometimes have to remove one or more policies. To remove a policy, you first remove it from Policy Manager. Then you save the new configuration to the Firebox.

1 From Policy Manager, click the policy.

2 In Policy Manager, click the **X** button on the Policy Manager toolbar.
You can also select Edit > Delete Policy.

3 When asked to confirm, click **Yes**.

4 Save the configuration to the Firebox and start the Firebox again. Select **File > Save > To Firebox**. Type the configuration passphrase. Select the **Save to Firebox** check box. Click **Save**.

Configuring Policy Properties

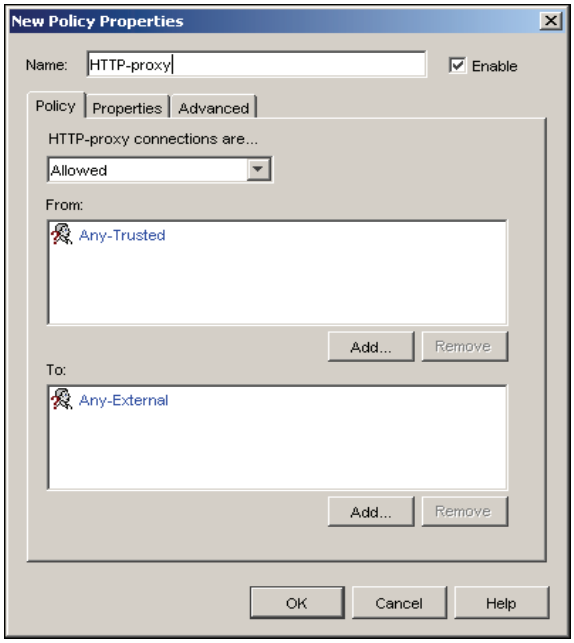
If you added a policy and want to change its properties, double-click the policy icon to open the **Edit Policy Properties** dialog box.

Setting access rules, sources, and destinations

You use the **Policy** tab to configure access rules for a given policy.

The **Policy** tab shows:

- If traffic that uses this policy is allowed or denied.
- Who uses this policy to start a connection with the users, hosts, and networks reachable through the Firebox®.
- The destinations for the traffic for this policy.



On the **From** list, you add the computers and networks that can send (or cannot send) network traffic with this policy. On the **To** list, you add computers and networks to which the Firebox routes traffic if it matches the policy specifications. For example, you could configure a ping packet filter to allow ping traffic from all computers on the external network to one web server on your optional network. For more information on the aliases that appear as options the From and To list, see "Working with Aliases" on page 73.

You can use these settings to configure how traffic is handled:

Allowed
: The Firebox allows traffic that uses this policy if it obeys the rules you set in the policy.

Denied
: The Firebox denies all traffic that matches this policy. You can configure it to record a log message when a computer tries to use this policy. It can also automatically add a computer or network that tries to start a connection with this policy to the Blocked Sites list (configured on the **Properties** tab).

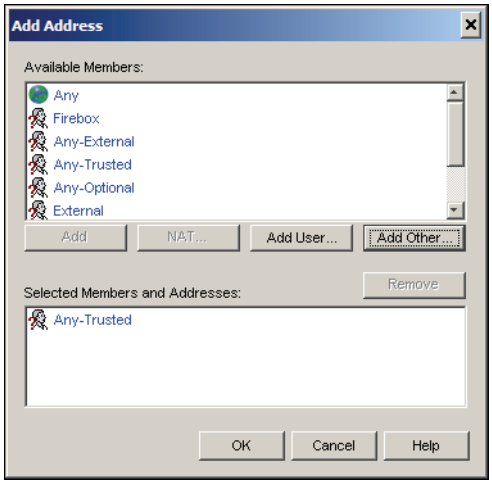
Denied (send reset)
: The Firebox denies all traffic that matches this policy. It can also automatically add a computer or network that tries to start a connection with this policy to the Blocked Sites list (configured on the **Properties** tab). The Firebox also sends a reset (RST) packet to tell the client that the session is refused and closed.

1 From the **Policy** tab, configure if connections are Allowed, Denied, or Denied (send reset).

2 To add members for the policy, click **Add** for the **From** or the **To** member list.

3 Use the **Add Address** dialog box to add a network, IP address, or specified user to a policy. Click either **Add User** or **Add Other.**

You can also select an item in the Available Members window and click **Add**, or double-click an item in this window. The Available Members list contains the aliases you add and the preconfigured aliases that Policy Manager gives.



4 If you selected **Add Other**, from the **Choose Type** drop-down list select the host range, host IP address, or network IP address to add. In the **Value** text box, type the correct network address, range, or IP address. Click **OK**.

The member or address appears in the Selected Members and Addresses list.

5 If you selected **Add User**, select the type of user or group, select the authentication server, and whether you want to add a user or group.

Do this again to add other members and addresses. Your policy can have more than one object in the **From** or **To** field.

6 Click **OK**.

Setting a proxy action

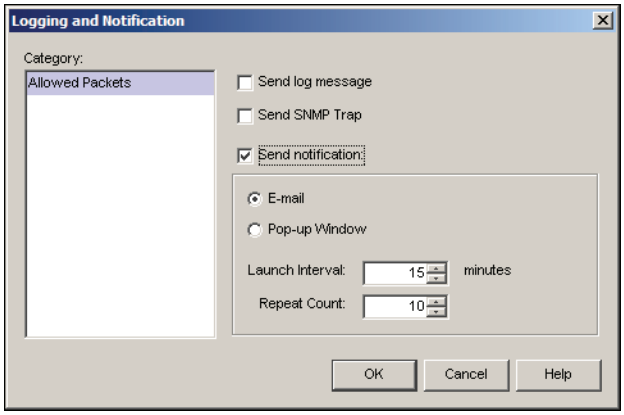
If you create a proxied policy, you can use the **Properties** tab of the **Policy Properties** dialog box to set a proxy action. For more information, see the "Configuring Proxied Policies" chapter.

This field is grayed out if you create a packet filter policy.

Setting logging properties

Use the **Properties** tab of the **Policy Properties** dialog box to set logging properties for a policy. You can configure the Firebox to record a log message when a policy denies packets. You can also set up notification when packets are allowed or denied.

1 From the **Properties** tab, click **Logging**.
The Logging and Notification dialog box appears.



2 Set the parameters and notification:

Enter it in the log

When you enable this check box, the Firebox sends a log message when it sees traffic of the type selected in the **Category** list. Domain name resolution on the Firebox can slow the time for the Firebox to send the log message to the log file. The default configuration of all policies is for the Firebox to send a log message when it denies a packet.

Send SNMP Trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The trap identifies the occurrence of a condition, such as a threshold that has exceeded its predetermined value.

Send notification

When you enable this check box, the Firebox sends a notification when it sees traffic of the type selected in the **Category** list. You set the notification parameters from the Log Server. For more information on the Log Server, see the "Logging and Notification" chapter.
You can configure the Firebox to do one of these actions:

- **E-mail** The Firebox sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Firebox makes a dialog box appear on the management station when the event occurs.
  You can control the time of notification, together with the Repeat Count. For information about how to use the Launch Interval and Repeat Count settings, see the subsequent section.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, with these parameters:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents multiple notifications in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log entry about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are configured as:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 a.m. and continues each minute. This starts the logging and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

If the policy you configured is a proxy, a **Proxy** drop-down list appears with the View/Edit Proxy and Clone Proxy icons. For information on how to use these options, see the "Configuring Proxied Policies" chapter in this guide.

Note

One policy manages either allowed or denied traffic, but not both. If you want the Firebox to send log messages for both allowed and denied traffic, you must use different policies for each.

Configuring static NAT

Static NAT is also known as port forwarding. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a specified public address and port. Static NAT changes this address to an address and port behind the firewall. For more information on NAT, see the "Working with Firewall NAT" chapter in this guide.

Because of how static NAT operates, it is available only for policies that use a specified port, which includes TCP and UDP. A policy that uses a different protocol cannot use incoming static NAT. The **NAT** button in the **Properties** dialog box of that policy does not operate. You also cannot use static NAT with the Any policy.

To help fight spam, many servers that receive e-mail do a reverse lookup of the source IP address the mail comes from. The receiving server does this to make sure that the sending server (the server sending the e-mail) is an authorized mail server for that domain. Because of this, we recommend that you use the external IP address of your Firebox as the MX record for your domain. An MX, or Mail exchange, record is a type of DNS record that sets how e-mail is routed through the Internet. MX records show the servers to send an e-mail to, and which server to send an e-mail to first, by priority.

Usually, connections that start from a trusted or optional network and go to the Internet show the external IP address of the Firebox as the source IP address of the packets. If the Firebox external IP address is not your domain's MX record IP address, some remote servers reject e-mail that you send. They do this because the SMTP session does not show your MX DNS record as the source IP address for the connection. If your Firebox does *not* use your MX record IP address as the external interface IP address, you can

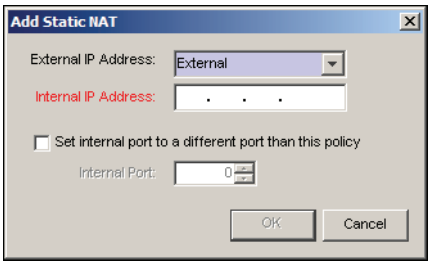
use a 1-to-1 NAT mapping to make outgoing e-mail connections show the correct source IP address. See the "Working with Firewall NAT" chapter for more information on 1-to-1 NAT.

1 In Policy Manager, double-click the policy icon.

2 From the **Connections are** drop-down list, select **Allowed**.
To use static NAT, the policy must let incoming traffic through.

3 Below the **To** list, click **Add**.
The Add Address dialog box appears.

4 Click **NAT**.
The Add Static NAT dialog box appears.



5 From the **External IP Address** drop-down list, select the "public" address to use for this policy.

6 Type the internal IP address.
The internal IP address is the destination on the trusted network.

7 If necessary, select the **Set internal port to different port than service** check box.
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host, but also to a different port. If you select the check box, type the different port number or use the arrow buttons in the Internal Port box.

8 Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.

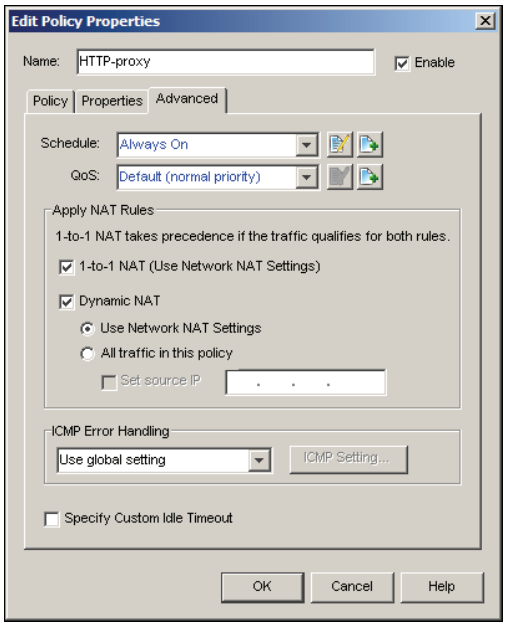
9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Properties** dialog box of the policy.

Note

Some organizations have more than one server that uses the same protocol (for example, two SMTP servers) and want to use static NAT for each server. You can do this if your Firebox is configured in routed mode and you have more than one public IP address to give to your Firebox. Set up two policies in Policy Manager. The first policy sets up static NAT between the primary external IP address of the Firebox and your first server. The second policy sets up static NAT between a secondary IP address of the Firebox external interface and your second server.

Setting advanced properties

You use the **Advanced** tab of the **Edit Policy Properties** dialog box to set a policy schedule, implement Quality of Service (QoS) settings, apply NAT rules, configure ICMP error handling for this policy, and set a custom idle time-out.



Setting a schedule

You can set an operating schedule for the policy. You can use the schedule templates in the **Schedule** drop-down list or create a custom schedule. For information, see the "Basic Configuration Setup" chapter in this guide.

Note that schedules can be shared by more than one policy.

Applying a Quality of Service (QoS) action

If you have Fireware® Pro on your Firebox, you can assign a Quality of Service action to the policy. Use the button on the far right to create a new QoS action. After you create a new QoS action, it appears in the **QoS** drop-down list. For more information, see "Creating QoS Actions" on page 209.

Note that these actions can be shared by more than one policy.

Applying NAT rules

You can apply Network Address Translation (NAT) rules to a policy:

1-to-1 NAT

With this type of NAT, the Firebox uses private and public IP ranges that you set, as described in "Using 1-to-1 NAT" on page 105.

Dynamic NAT

With this type of NAT, the Firebox maps private IP addresses to public IP addresses. Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the Firebox. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

You also have the option to set a dynamic NAT source IP address for any policy that uses

dynamic NAT. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. You would most often do this to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the Firebox's external interface is not the same as your MX record IP address.

1-to-1 NAT rules have higher precedence than dynamic NAT rules

Note

If you use multi-WAN, you cannot use the **Set Source IP** option. Use this option only when your Firebox uses a single external interface.

Setting ICMP error handling

You can set the ICMP error handling settings associated with the policy.

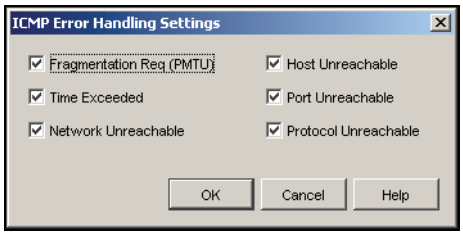
From the drop-down list, select:

Use global setting

Use the global ICMP error handling setting set for the Firebox. For information on this global setting, see "ICMP error handling" on page 40.

Specify setting

Configure a parameter that overrides the global setting. Click **ICMP Setting**. From the **ICMP Error Handling Settings** dialog box, select the check boxes to configure individual settings. For information on these settings, see "ICMP error handling" on page 40.



Setting a custom idle time-out

To set an idle time-out, click **Specify Custom Idle Timeout** and click the arrows to set the number of seconds before time-out. This setting overrides the idle time-out of the policy.

Setting Policy Precedence

Precedence is the sequence in which the Firebox® examines network traffic and applies a policy rule. The Firebox routes the traffic that uses the rules for the first policy that the traffic matches. Fireware® Policy Manager automatically sorts policies from the most detailed to the most general. You can also manually set the precedence.

Using automatic order

Fireware Policy Manager automatically sorts policies from the most detailed to the most general. Each time you add a policy, Policy Manager compares the new rule with all the rules in your configuration file. To set the precedence, Policy Manager uses these criteria:

1 Protocols set for the policy type

2 Traffic rules of the **To** field
3 Traffic rules of the **From** field
4 Firewall action
5 Schedule
6 Alphanumeric sequence based on policy type
7 Alphanumeric sequence based on policy name

Comparing policy type

Policy Manager uses these criteria in sequence to compare two policies until it finds that the policies are equal or that one is more detailed than the other:

1 An Any policy always has the lowest precedence. For more information about the Any policy, see "Any" on page 233.
2 Check the number of TCP 0 (any) or UDP 0 (any) protocols. The policy with the smaller number has higher precedence.
3 Check the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.
4 Count the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.
5 Score the protocols based on their IP protocol value. The policy with the smaller score has higher precedence.

If Policy Manager cannot set the precedence when it compares the policy type, it examines traffic rules.

Comparing traffic rules

Policy Manager uses these criteria in sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy. It assigns higher precedence to the policy with the most detailed traffic rule. The list of traffic rules from most detailed to the most general is:

1 Host address
2 IP address range (smaller than the subnet being compared to)
3 Subnet
4 IP address range (larger than the subnet being compared to)
5 Authentication user
6 Authentication group
7 Interface, Firebox
8 Any-External, Any-Trusted, Any-Optional
9 Any

For example, compare these two policies:

HTTP-1
From: Trusted, user1

HTTP-2
From: 10.0.0.1, Any-Trusted

"Trusted" is the most general entry for HTTP-1. "Any-Trusted" is the most general entry for HTTP-2. Because "Trusted" is within "Any-Trusted," HTTP-1 is the more detailed traffic rule. This is correct despite the fact that HTTP-2 includes an IP address. This is because Policy Manager uses these criteria in

sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy.

If Policy Manager cannot set the precedence when it compares the traffic rules, it examines the firewall actions.

Comparing firewall actions

Policy Manager compares the firewall actions of two policies to set precedence. Precedence of firewall actions from highest to lowest is:

1 Denied or Denied (send reset)

2 Allowed proxy

3 Allowed filter

If Policy Manager cannot set the precedence when it compares the firewall actions, it examines the schedules.

Comparing schedules

Policy Manager compares the schedules of two policies to set precedence. Precedence of schedules from highest to lowest is:

1 Always off

2 Sometimes on

3 Always on

If Policy Manager cannot set the precedence when it compares the schedules, it examines the policy names.

Comparing type and names

If the two policies do not match any other precedence criteria, Policy Manager sorts the policies in alphanumeric sequence. First it uses the policy type. Then it uses the policy name. Because no two policies can be the same type and have the same name, this is the last criteria for precedence.

Setting precedence manually

To switch to manual-order mode, select **View > Auto-order mode** so that the checkmark disappears. You are asked to confirm if you want to switch to auto-order mode.

To change the order of policies:

- Select the policy whose order you want to change. Click the up or down arrow on the far right side of the Policy Manager toolbar.

or

- Select the policy whose order you want to change and drag it to its new location.

CHAPTER 13

Configuring Proxied Policies

Proxy filters do much more than packet filters. A proxy examines the contents of a packet, not only the header. As a result, the proxy finds forbidden content hidden or embedded in the data payload. For example, an SMTP proxy examines all incoming SMTP packets (e-mail) to find forbidden content, such as executable programs or files written in scripting languages. Attackers frequently use these methods to send computer viruses. The SMTP proxy knows these content types are not allowed, while a packet filter cannot detect the unauthorized content in the packet's data payload.

WatchGuard® proxies also look for application protocol anomalies and stop packets that are not made correctly. If an SMTP packet is not made correctly or contains unexpected content, it cannot go through the Firebox®.

Proxy policies operate at the application, network, and transport protocol levels. Packet filter policies operate at only the network and transport protocol level. In other words, a proxy gets each packet, removes the network layer, and examines its payload. The proxy then puts the network information back on the packet and sends it to its destination on your trusted and optional networks. This adds more work for your firewall for the same volume of network traffic. But a proxy uses methods that packet filters cannot to catch dangerous packets.

Defining Rules

A ruleset is a group of rules based on one feature of a proxy. When you configure a proxy, you can see the rulesets for that proxy in the **Categories** list. The rulesets you see change when you change the proxy action on the **Properties** tab of a proxy configuration window.

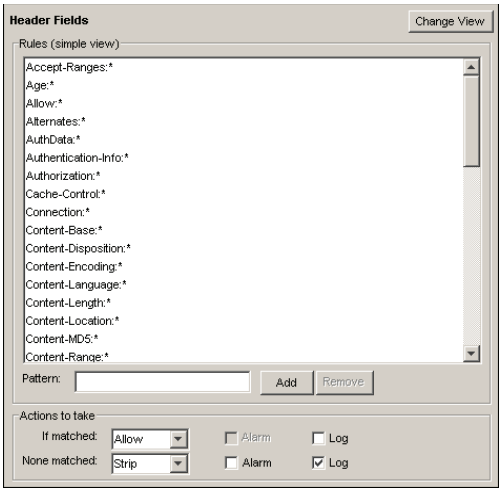
A proxy can have more than one proxy action associated with it. For example, you can use one ruleset for packets sent to an e-mail server protected by the Firebox® and a different ruleset to apply to e-mail messages being sent out through the Firebox to the Internet. You can use the existing proxy actions, or clone an existing proxy action and change it to create a new proxy action.

A rule includes a type of content, pattern, or expression and the action the Firebox does when a component of the packet's content matches a rule. Rules also include settings for when the Firebox sends alarms or if it sends events to the log file.

For most proxy features, the Firebox has a preinstalled ruleset. But you can edit the rules in a ruleset to change the action for the rules. You can also add your own rules.

The fields you use for these rule definitions look the same for each category of ruleset. The simple view is shown below. You can also select **Change View** to see the advanced view.

Use the advanced view to improve the matching function of a proxy. In advanced view, you can configure exact match and Perl-compatible regular expressions. In simple view, you can configure wildcard pattern matching with simple regular expressions.



Adding rulesets

From the simple view, do these steps to add new rules:

1 In the **Pattern** text box, type a pattern that uses simple regular expression syntax.
The wildcard for zero or more than one character is "*".
The wildcard for one character is "?".

2 Click **Add**.
The new rule appears in the Rules box.

3 In the **Actions to take** section, the **If matched** drop-down list sets the action to do if the contents of a packet match one of the rules in the list. The **None matched** drop-down list sets the action to do if the contents of a packet do not match a rule in the list. Below is a list of all possible actions. The actions **Strip** and **Lock** apply only to signature-based intrusion prevention actions.

Allow
Allows the connection.

Deny
Denies a specific request but keeps the connection if possible.

Drop
Denies the specific request and drops the connection.

Block
Denies the request, drops the connection, and adds the source host to the Blocked Sites list. For more information on blocked sites, see "Setting Blocked Sites" on page 135.

Strip
Removes an attachment from a packet and discards it. The other parts of the packet are sent through the Firebox to its destination.

Lock

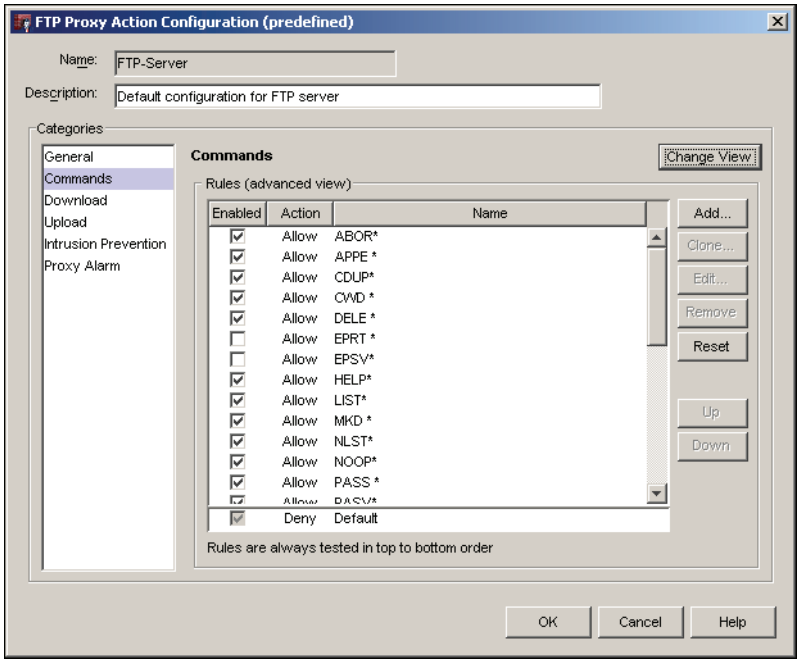
Locks an attachment, and wraps it so that it cannot be opened by the user. Only the administrator can unlock the file.

4 An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box to configure an alarm for this event. To set the options for the alarm, select **Proxy Alarm** from the **Categories** list on the left side of a Proxy Configuration window. You can send an SNMP trap, send e-mail, or open a pop-up window.

5 Use the **Log** check box to write a traffic log for this event.

Using the advanced rules view

To see a detailed view of the current rules, click **Change View**. The advanced view shows the action for each rule. It also has buttons you can use to edit, clone (use an existing rule definition to start a new one), delete, or reset rules. To go back to the simple view, click **Change View** again. You cannot go back to simple view if the enabled rules have different action, alarm, and log settings. In this case, you must continue to use the advanced view.



Changing the precedence of rules

The Firebox uses these guidelines to apply rules:

- It does the rules in sequence from the top to the bottom of the window.
- When a filtered item matches a rule, the Firebox does the related traffic action.
- Content can match more than one of the rules or the default rule, but only the first rule is used.
- The Firebox uses the default rule if no other rule applies. It is always the last rule that the Firebox applies to the content.

To change the sequence of rules, you must use the advanced view:

1 Click **Change View** to see the advanced view of created rules.

2 Select a rule to move up or down in the list. Click the **Up** or **Down** button to move the rule up or down in the list.

Customizing Logging and Notification for Proxy Rules

An alarm, log message, or notification is a mechanism to tell a network administrator about network traffic that does not match the criteria for allowed traffic. For example, if traffic is more than a threshold value, you can configure the Firebox® to send you an e-mail message. You can set alarm, log message, and notification properties for each packet filter and proxy policy. You can also set alarm and log message properties for a proxy rule.

Configuring log messages and notification for a proxy policy

1 Double-click the policy icon to open the **Policy Properties** dialog box.

2 Click the **Properties** tab. Click **Logging**.
The Logging and Notification dialog box appears.

3 Set the parameters to agree with the requirements of your security policy.

Configuring log messages and alarms for a proxy rule

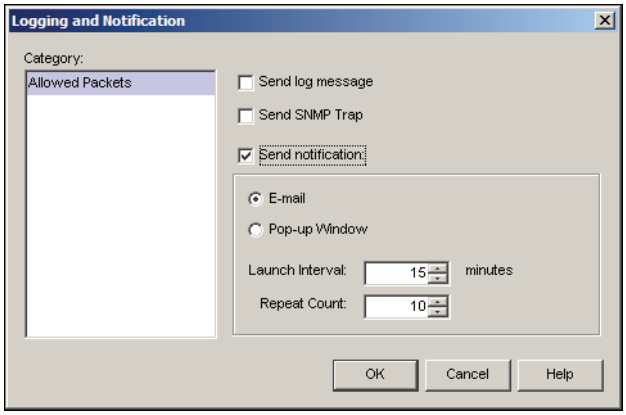
1 Double-click the policy icon to open the **Policy Properties** dialog box.

2 Click the **Properties** tab. From the **Proxy** drop-down list, select the proxy action to configure.

3 Select **Proxy Alarms** from the **Category** list. For more information about the parameters, see the subsequent section.
There are more log messages and notification options available with signature-based intrusion prevention services. These options are examined in the chapter "Using Signature-Based Security Services."

Using dialog boxes for alarms, log messages, and notification

The dialog boxes for alarms, log messages, and notification in proxy definitions have most or all of these fields:



Enter it in the log

When you enable this check box, the Firebox sends a traffic log message to the Log Server when this event occurs. The default configuration of all policies is for the Firebox to send a log message when it denies a packet.

Send SNMP Trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The SNMP trap shows when the traffic matches a condition such as a property that is more than its threshold value. Note that the bindings section in the SNMP trap is blank if the trap occurs when SNMP starts or stops, such as with a reset, restart, or failover.

Send notification

When you enable this check box, the Log Server sends a notification when this event occurs. You can configure the Log Server to do one of these actions:

- **E-mail** The Log Server sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Log Server makes a dialog box appear on the management station when the event occurs.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, as follows:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log message about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are set up as follows:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 AM and continues each minute. This starts the log and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

Configuring the SMTP Proxy

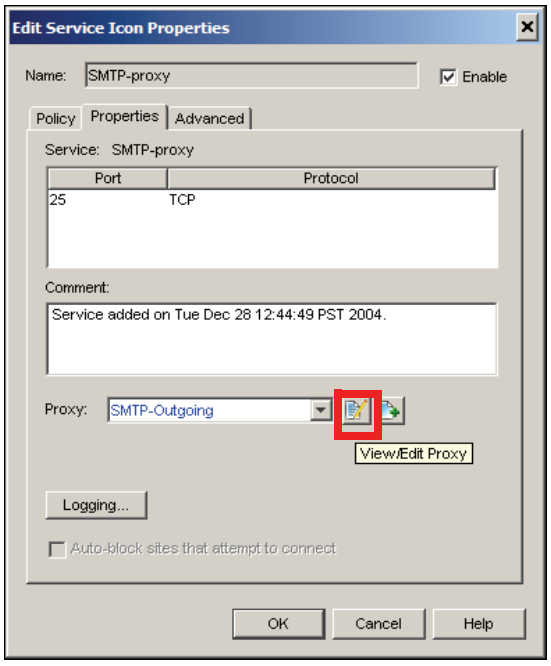
You use the SMTP proxy to control e-mail messages and e-mail content. The proxy scans SMTP messages for a number of filtered parameters, and compares them against the rules set in the proxy configuration. To configure the SMTP proxy:

1 Add the SMTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 66.

2 Double-click the SMTP icon and select the **Properties** tab.
The Edit Policy Properties dialog box appears and shows the General Settings information.

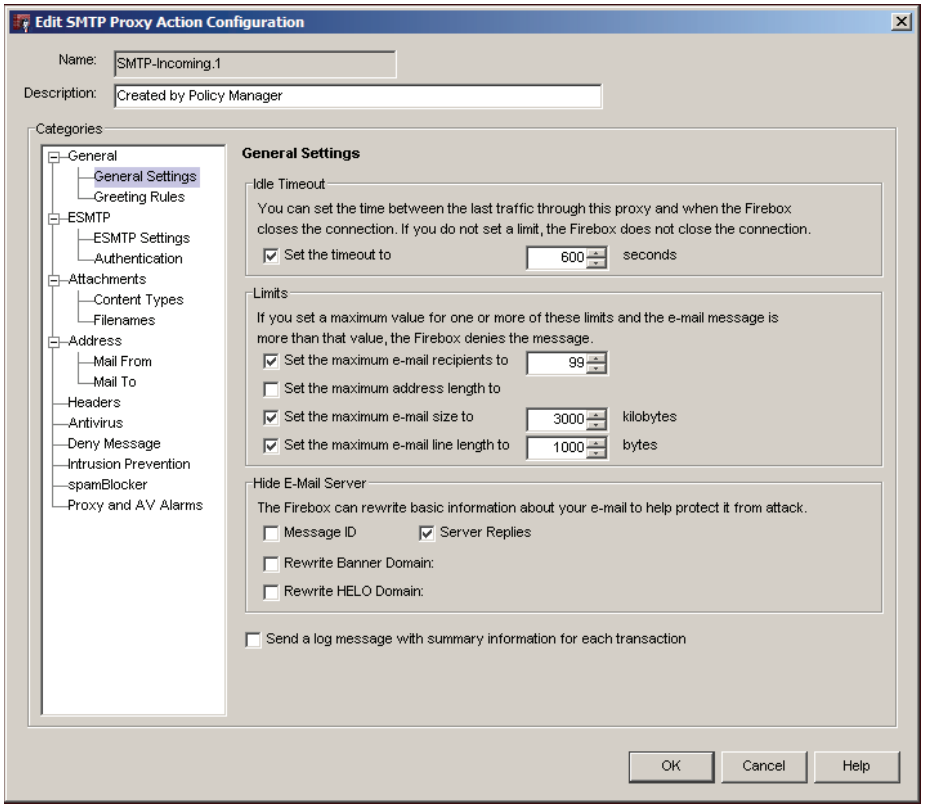
3 In the **Proxy** drop-down list, select to configure SMTP-Incoming or SMTP-Outgoing.
You can also clone a proxy action to create a new proxy action.

4 Click the **View/Edit Proxy** icon.



Configuring general settings

You use the **General Settings** fields to configure basic SMTP proxy parameters such as idle time-out and message limits.



Idle timeout

You can set the length of time an incoming SMTP connection can idle before the connection times out. The default value is 600 seconds (10 minutes). For no time-out, clear the **Set the timeout to** check box.

Maximum e-mail recipients

With the **Set the maximum e-mail recipients to** check box, you can set the maximum number of e-mail recipients to which a message can be sent. The Firebox® counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you use the default value of 50 and there is a message for 52 addresses, the first 50 addresses get the e-mail message. The last two addresses do not get a copy of the message. A distribution list appears as one SMTP e-mail address (for example, support@watchguard.com). The Firebox counts this as one address.

You can use this feature to decrease spam e-mail because spam usually includes a large recipient list. Be careful when you do this because you can also deny legitimate e-mail.

Maximum address length

With the **Set the maximum address length to** check box, you can set the maximum length of e-mail addresses.

Maximum e-mail size

With the **Set the maximum e-mail size to** check box, you can set the maximum length of an incoming SMTP message. Most e-mail is sent as 7-bit ASCII text. The exceptions are Binary MIME

and 8-bit MIME. 8-bit MIME content (for example, MIME attachments) is encoded with standard algorithms (Base64 or quote-printable encoding) to enable them to be sent through 7-bit e-mail systems. Encoding can increase the length of files by as much as one third. To allow messages as large as 1000 bytes, you must set this field to a minimum of 1334 bytes to make sure all e-mail gets through. The default value is 3,000,000 bytes (3 million bytes).

Maximum e-mail line length

With the **Set the maximum e-mail line length to** check box, you can set the maximum line length for lines in an SMTP message. Very long line lengths can cause buffer overflows on some e-mail systems. Most e-mail clients and systems send short line lengths, but some web-based e-mail systems send very long lines. The default value is 1024.

Hide E-mail Server

Select the **Message ID** and **Server Replies** check boxes to replace MIME boundary and SMTP greeting strings in e-mail messages. These are used by hackers to identify the SMTP server vendor and version.

If you have an e-mail server and use the SMTP-Incoming proxy action, you can have the SMTP proxy replace the domain shown in your SMTP server banner with a domain name you select. To do this, select the **Rewrite Banner Domain** check box and type the domain name you want to use in your banner in the text box that appears. For this to occur, you must also have the **Server Replies** check box selected.

If you use the SMTP-Outgoing proxy action, you can have the SMTP proxy replace the domain shown in the HELO or EHLO greetings. A HELO or EHLO greeting is the first part of an SMTP transaction, when your e-mail server announces itself to a receiving e-mail server. To do this, select the **Rewrite HELO Domain** check box and type the domain name you want to use in your HELO or EHLO greeting in the text box that appears.

Send a log message

Select the **Send a log message** check box to send a log message for each connection request through SMTP. For Historical Reports to create accurate reports on SMTP traffic, you must select this check box.

Greeting rules

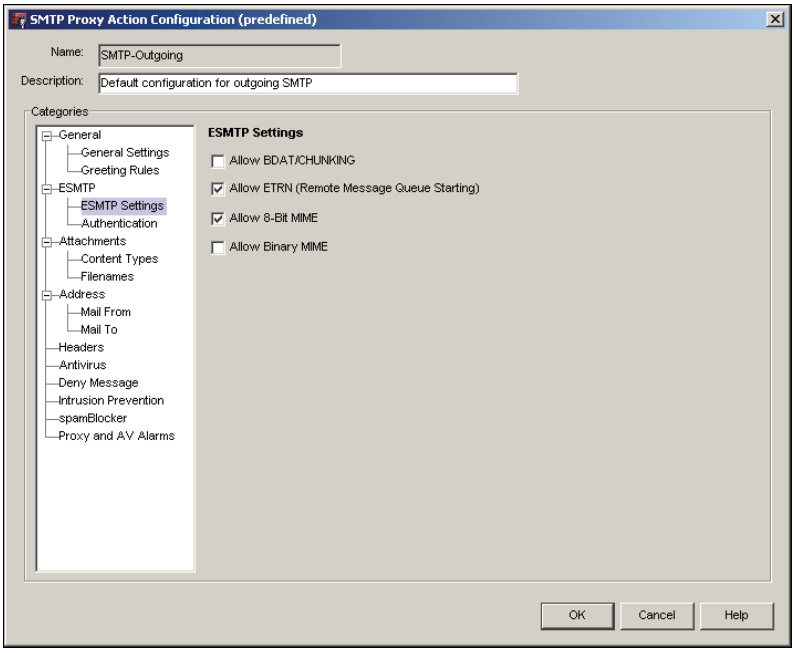
The proxy examines the initial HELO/EHLO responses during the SMTP session initialization. The default rules for the SMTP-Incoming proxy action make sure that packets with greetings that are too long, or include characters that are not correct or expected, are denied.

Configuring ESMTP parameters

You use the **ESMTP Settings** fields to set the filtering for ESMTP content. Although SMTP is widely accepted and widely used, some parts of the Internet community have found a need to extend SMTP to

allow more functionality. ESMTP gives a method for functional extensions to SMTP, and for clients who support extended features to know each other.

1 From the **Categories** section, select **ESMTP Settings**.



Allow BDAT/CHUNKING

Select to allow BDAT/CHUNKING. This enables large messages to be sent more easily through SMTP connections.

Allow ETRN (Remote Message Queue Starting)

This is an extension to SMTP that allows an SMTP client and server to interact to start the exchange of message queues for a given host.

Allow 8-Bit MIME

Select to allow 8-bit MIME, if the client and host give support to the extension. The 8-bit MIME extension allows a client and host to exchange messages made up of text that has octets which are not of the US-ASCII octet range (hex 00-7F, or 7-bit ASCII) that uses SMTP.

Allow Binary MIME

Select to allow the Binary MIME extension, if the sender and receiver accept it. Binary MIME prevents the overhead of base64 and quoted-printable encoding of binary objects sent that use the MIME message format with SMTP. We do not recommend you select this option as it can be a security risk.

Configuring authentication rules

This ruleset allows a number of ESMTP authentication types. The default rule denies all other authentication types. The RFC that tells about the SMTP authentication extension is RFC 2554.

1 From the **Categories** section, select **Authentication**.

2 Do the steps used to create rules. For more information, see “Defining Rules” on page 79.

Defining content type rules

You use the ruleset for the SMTP-Incoming proxy action to set values for incoming SMTP content filtering. You use the ruleset for the SMTP-Outgoing proxy action to set values for outgoing SMTP content filtering.

1 From the **Categories** section, select **Content Types**.

2 Do the steps used to create rules. For more information, see "Defining Rulesets" on page 79.

Defining file name rules

You use the ruleset for the SMTP-Incoming proxy action to put limits on file names for incoming e-mail attachments. You use the ruleset for the SMTP-Outgoing proxy action to put limits on file names for outgoing e-mail attachments.

1 From the **Categories** section, select **Filenames**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Configuring the Mail From and Mail To rules

The **Mail From** ruleset can put limits on e-mail to allow e-mail into your network only from specified senders. The default configuration is to allow e-mail from all senders.

The **Mail To** ruleset can put limits on e-mail to allow e-mail out of your network only to specified recipients. The default configuration allows e-mail to all recipients out of your network. On an SMTP-Incoming proxy action, you can use the Mail To ruleset to prevent people from using your e-mail server for e-mail relaying. To do this, make sure that all domains your e-mail server accepts e-mail for appear in the rule list. Then, make sure the **Action to Take** if **None Matched** is set to **Deny**. Any e-mail with an address that does not match the listed domains is denied.

You can also use the **Rewrite As** feature included in this rule configuration dialog box to have the Firebox change the From and To components of your e-mail address to a different value. This feature is also known as "SMTP masquerading."

1 From the **Categories** section, select **Mail From** or **Mail To**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Defining header rules

Header rulesets allow you to set values for incoming or outgoing SMTP header filtering.

1 From the **Categories** section, select **Headers**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Defining antivirus responses

The fields in this dialog box set the actions necessary if a virus is found in an e-mail message. It also sets actions for when an e-mail message contains an attachment that is too large or that the Firebox cannot scan.

Although you can use the proxy definition screens to activate and configure Gateway AntiVirus, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the antivirus screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Changing the deny message

The Firebox gives a default deny message that replaces denied content. You can replace that deny message with one that you write. You can write a custom deny message with standard HTML. The first line of the deny message is a section of the HTTP header. There must be an empty line between the first line and the body of the message.

1 From the **Categories** section, select **Deny Message**.

2 Type the deny message in the deny message box. You can use these variables:

%(reason)%
Puts the cause for the Firebox to deny the content.

%(type)%
Puts the type of content that was denied.

%(filename)%
Puts the file name of the denied content.

%(virus)%
Puts the name or status of a virus, for Gateway AntiVirus users only.

%(action)%
Puts the name of the action taken: lock, strip, and so on.

%(recovery)%
Allows you to set the text to fill this sentence: "Your network administrator %(recovery)% this attachment.

Configuring the IPS (Intrusion Prevention System) for SMTP

Hackers use many methods to attack computers on the Internet. The function of these attacks is to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as *intrusions*.

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Configuring spamBlocker

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard® spamBlocker™ option increases your capacity to catch spam at the edge of your network when it tries to come into your system.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the spamBlocker screens in the proxy definition, see the chapter "Using spamBlocker."

Configuring proxy and antivirus alarms for SMTP

You can set the action the Firebox does when proxy or antivirus (AV) alarm events occur:

1 From the **Categories** section, select **Proxy and AV Alarms.**

2 For information on fields in the **Proxy/AV Alarm Configuration** section, see "Using dialog boxes for alarms, log messages, and notification" on page 164.

Configuring the FTP Proxy

File Transfer Protocol (FTP) is the protocol used to move files on the Internet. Like SMTP and HTTP, FTP uses TCP/IP protocols to enable data transfer. You usually use FTP to download a file from a server on the Internet or to upload a file to a server.

1 Add the FTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 66.

2 Double-click the FTP icon and select the **Policy** tab.

3 Select **Allowed** from the **FTP proxy connections are** drop-down list.

4 Select the **Properties** tab.

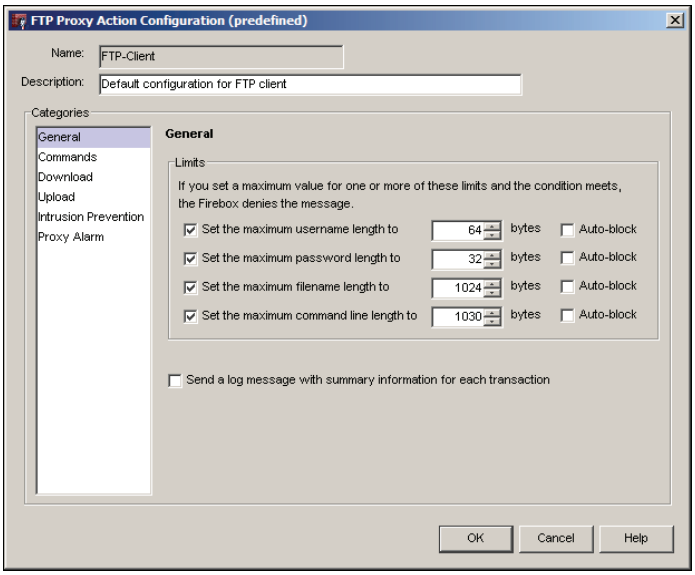
5 In the **Proxy** drop-down list, select to configure the proxy action for FTP-Client or FTP-Server.

6 Click the **View/Edit Proxy** icon.

Configuring general settings

You use the **General** fields to configure basic FTP parameters including maximum user name length.

1 From the **Categories** section, select **General**.



2 To set limits for FTP parameters, select the applicable check boxes. These settings help to protect your network from buffer overflow attacks. If you set a check box to 0 bytes, the Firebox® does not use the parameter. Use the arrows to set the limits:

Maximum user name length
Sets a maximum length for user names on FTP sites.

Maximum password length
Sets a maximum length for passwords used to log in to FTP sites.

Maximum file name length
Sets the maximum file name length for files to upload or download.

Maximum command line length
Sets the maximum length for command lines used on FTP sites.

3 For each setting, you can set or clear the **Auto-block** check box next to it. If someone tries to connect to an FTP site and exceeds a limit whose **Auto-block** check box is selected, the computer that sent the commands is added to the temporary Blocked Sites list.

4 To create a log message for each transaction, select the **Send a log message with summary information for each transaction** check box.

Defining commands rules for FTP

FTP has a number of commands to manage files. You can write rules to put limits on some FTP commands. Use the FTP-Server proxy action to put limits on commands that can be used on an FTP server protected by the Firebox. Use the FTP-Client proxy action to put limits on commands that users protected by the Firebox can use when they connect to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

1 From the **Categories** section, select **Commands**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Setting download rules for FTP

Download rules control the file names, extensions, or URL paths that users can use FTP to download. Use the FTP-Server proxy action to control download rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set download rules for users connecting to external FTP servers. To add download rulesets:

1 From the **Categories** section, select **Download**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Setting upload rules for FTP

Upload rulesets control the file names, extensions, or URL paths that users can use FTP to upload. Use the FTP-Server proxy action to control upload rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set upload rules for users connecting to external FTP servers. The default configuration of the FTP-Client is to allow all files to be uploaded. To create upload rulesets:

1 From the **Categories** section, select **Upload.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Enabling intrusion prevention for FTP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Configuring proxy alarms for FTP

An alarm is a mechanism to tell a network administrator when network traffic matches criteria for suspicious traffic or content. When an alarm event occurs, the Firebox does an action that you configure. For example, you can set a threshold value for file length. If the file is larger than the threshold value, the Firebox can send a log message to the Log Server.

1 From the **Categories** section, select **Proxy Alarm**.

2 For information on fields in the **Proxy Alarm Configuration** section, see "Using dialog boxes for alarms, log messages, and notification" on page 164.

Configuring the HTTP Proxy

The HTTP proxy is a high performance content filter. It examines web traffic to identify suspicious content which can be a virus, spyware, or other types of intrusion. It can also protect your web server from attacks from the external network. You can configure the HTTP proxy to:

- Allow only content that matches RFC requirements for web servers and clients
- Select which types of MIME content the Firebox® allows into your network
- Block Java, ActiveX, and other code types
- Examine the HTTP header to make sure it is not from a known source of suspicious content

1 Add the HTTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see"Adding Policies" on page 66.

2 Select the **Properties** tab.

3 In the **Proxy** drop-down list, select to configure the HTTP-Client or HTTP-Server proxy action. Use the HTTP-Server proxy action (or an incoming proxy action you create based on the HTTP-Server proxy action) to protect a web server. Use HTTP-Client, or an outgoing proxy action, to filter HTTP requests from users behind the Firebox.

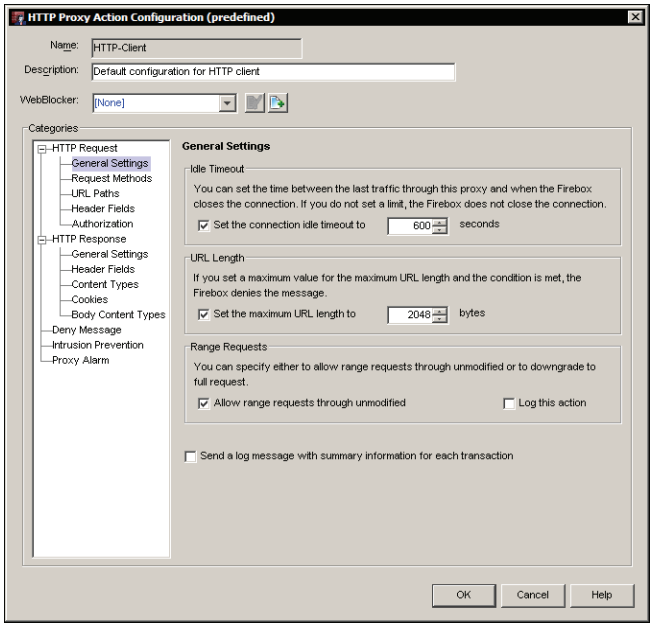
4 Click the **View/Edit Proxy** icon.
You can also clone a proxy action to create a new proxy action.

Configuring settings for HTTP requests

You can configure general settings for HTTP requests. You can also see and edit the HTTP request rulesets included in a proxy action. To get access to these settings, click **HTTP Request** in the **Categories** list on the left of the proxy configuration.

Configuring general settings for HTTP requests

You use the **General Settings** fields to configure basic HTTP parameters such as idle time-out and URL length.



Idle Timeout

Controls how long the HTTP proxy waits for the web client to make a request for something from the external web server after it starts a TCP/IP connection or after the earlier request, if there was one, for the same connection. If it goes longer than the setting, the HTTP proxy closes the connection. The default value is 600 seconds.

URL Length

Sets the maximum length of the path component of a URL. This does not include the "http:\\" or host name. Control of the URL length can help to prevent buffer overflow attacks.

Range requests

Range requests allow a client to request subsets of the bytes in a web resource instead of the full content. For example, this is useful when you want only some sections of a large Adobe file. You can select a range request to prevent the download of unnecessary pages. If you allow range requests through the Firebox and download a file infected with a virus whose signature is divided between two pages, antivirus software will not detect the virus. To allow range requests can make downloads occur more quickly, but it is not as safe.

Send a log message with summary information for each transaction

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTP proxied connections in Historical Reports.

Setting HTTP request methods

Most browser HTTP requests are in one of two categories: GET and POST operations. Browsers usually use GET operations to download objects such as a graphic, HTML data, or Flash data. More than one GET is usually sent by a client computer for each page, because web pages usually contain many different elements. The elements are put together to make a page that appears as one page to the end user.

Browsers usually use POST operations to send data to a web site. Many web pages get information from the end user such as location, e-mail address, and name. If you disable the POST command, the Firebox denies all POST operations to web servers on the external network. This features can prevent your users from sending information to a web site on the external network.

The HTTP proxy supports request methods: HEAD, GET, POST, OPTIONS, PUT, and DELETE. (For HTTP-Server, the proxy supports these request methods by default: HEAD, GET, and POST. OPTIONS, PUT, and DELETE are added but are disabled.) You can also add CONNECT and TRACE, but no other request methods are supported at this time. If you configure a rule to allow other request methods and your browser tries to use them, you get an error with the text: "Method unsupported."

1 From the **Categories** section, select **Request Methods**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request URL paths

You use URL path rules to filter the content of the host, path, and query-string components of a URL. Here are examples of how to block content using HTTP request URL paths:

- To block all pages that have the host name www.test.com, type the pattern: www.test.com*
- To block all paths containing the word "sex", on all web sites: *sex*
- To block URL paths ending in "*.test", on all web sites: *.test

Note

Usually, if you filter URLs with the HTTP request URL path ruleset, you must configure a complex pattern that uses full regular expression syntax and the advanced view of a ruleset. It is easier and gives better results to filter based on header or body content type than it is to filter by URL path.

1 From the **Categories** section, select **URL paths**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request header fields

This ruleset supplies content filtering for the full HTTP header. By default, the Firebox uses exact matching rules to strip Via and From headers, and allows all other headers. This ruleset matches against the full header, not only the name. Thus, to match all values of a header, type the pattern: "[*header name*]:*". To match only some values of a header, replace the asterisk (*) wildcard with a pattern. If your pattern does not start with an asterisk (*) wildcard, include one space between the colon and the pattern when typing in the **Pattern** text box. For example, type: [*header name*]: [*pattern*] and not [*header name*]:[*pattern*].

Note that the default rules do not strip the Referer header, but do include a disabled rule to strip this header. To enable the rule, select **Change View**. Some web browsers and software applications must use the Referer header to operate correctly.

1 From the **Categories** section, select **Header Fields**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request authorization

This rule sets the criteria for content filtering of HTTP Request Header authorization fields. When a web server starts a "WWW-Authenticate" challenge, it sends information about which authentication methods it can use. The proxy puts limits on the type of authentication sent in a request. It uses only the

authentication methods that the web server accepts. With a default configuration, the Firebox allows Basic, Digest, NTLM, and Passport1.4 authentication, and strips all other authentication.

1 From the **Categories** section, select **Authorization**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Configuring general settings for HTTP responses

You use the General Settings fields to configure basic HTTP parameters such as idle time-out and limits for line and total length. If you set a check box to 0 bytes, the Firebox does not check the parameter.

1 From the **Categories** section, select **General Settings**.

2 To set limits for HTTP parameters, select the applicable check boxes. Use the arrows to set the limits:

Idle timeout
: Controls how long the Firebox HTTP proxy waits for the web server to send the web page. The default value is 600 seconds.

Maximum line length
: Controls the maximum allowed length of a line of characters in the HTTP response headers. Use this property to protect your computers from buffer overflow exploits.

Maximum total length
: Controls the maximum length of the HTTP response headers. If the total header length is more than this limit, the HTTP response is denied. The default value is 0 (no limit).

Setting header fields for HTTP responses

This property controls which HTTP response header fields the Firebox allows. RFC 2616 includes many of the HTTP response headers that are allowed in the default configuration. For more information, see:

http://www.ietf.org/rfc/rfc2616.txt

1 From the **Categories** section, select **Header Fields**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Setting content types for HTTP responses

When a web server sends HTTP traffic, it usually adds a MIME type to the response. The HTTP header on the data stream contains this MIME type. It is added before the data is sent.

This ruleset sets rules for looking for content type (MIME type) in HTTP response headers. By default the Firebox allows some safe content types, and denies MIME content that has no specified content type. Some web servers supply incorrect MIME types to get around content rules.

1 From the **Categories** section, select **Content Types**.

2 Do the steps used to create rulesets. For more information, see "Defining Rules" on page 161.

Setting cookies for HTTP responses

HTTP cookies are small files of alphanumeric text put by web servers on web clients. Cookies monitor the page a web client is on to enable the web server to send more pages in the correct sequence. Web servers also use cookies to collect information about an end user. Many web sites use cookies for authentication and other legitimate functions and cannot operate correctly without cookies.

This ruleset gives you control of the cookies in HTTP responses. You can configure rules to strip cookies, based on your network requirements. The default rule for the HTTP-Server and HTTP-Client proxy action allows all cookies.

The Cookies ruleset looks for packets based on the domain associated with the cookie. The domain can be specified in the cookie. If there is no domain in the cookie, the proxy uses the host name in the first request. Thus, to block all cookies for nosy-adware-site.com, add a rule with the pattern: "*.nosy-adware-site.com".

1 From the **Categories** section on the left, select **Cookies.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Setting HTTP body content types

This ruleset gives you control of the content in an HTTP response. The Firebox is configured to deny Java applets, Zip archives, Windows EXE/DLL files, and Windows CAB files. The default proxy action for outgoing HTTP requests (HTTP-Client) allows all other response body content types. We recommend that you examine the file types that are used in your organization and allow only those file types that are necessary for your network.

1 From the **Categories** section, select **Body Content Types.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Defining antivirus responses for HTTP

The fields on this dialog box set the actions necessary if a virus is found in an e-mail message. It also sets actions for when an e-mail message contains an attachment that is too large or that the Firebox cannot scan.

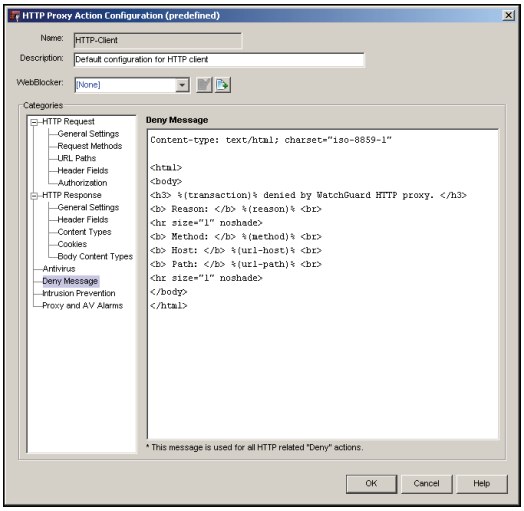
Although you can use the proxy definition screens to activate and configure Gateway AntiVirus, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the antivirus screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Changing the deny message

The Firebox gives a default deny message that replaces the content that is denied. You can replace that deny message with one that you write. You can customize the deny message with standard HTML. The

first line of the deny message is a component of the HTTP header. There must be an empty line between the first line and the body of the message.

1 From the **Categories** section, select **Deny Message**.



2 Type the deny message in the deny message box. You can use these variables:

%(transaction)%
: Puts "Request" or "Response" to show which side of the transaction caused the packet to be denied.

%(reason)%
: Puts the reason the Firebox denied the content.

%(method)%
: Puts the request method from the denied request.

%(url-host)%
: Puts the server host name from the denied URL. If no host name was included, the IP address of the server is given.

%(url-path)%
: Puts the path component of the denied URL.

Enabling intrusion prevention for HTTP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Defining proxy and antivirus alarms for HTTP

Use these settings to set criteria for a notification event:

1 From the **Categories** section, select **Proxy and AV Alarms.**

2 Do the steps in "Using dialog boxes for alarms, log messages, and notification" on page 164.

Configuring the DNS Proxy

With the Domain Name System (DNS), you can get access to a web site with an easy-to-remember "dot-com" name. DNS finds the Internet domain name (for example WatchGuard.com) and changes it to an IP address. The DNS proxy protects your DNS servers from TSIG, NXT, and other DNS attacks. To add the DNS proxy to your Firebox® configuration:

1 Add the DNS proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 66.

2 Double-click the DNS icon and select the **Policy** tab.

3 Select **Allowed** from the **DNS proxy connections are** drop-down list.

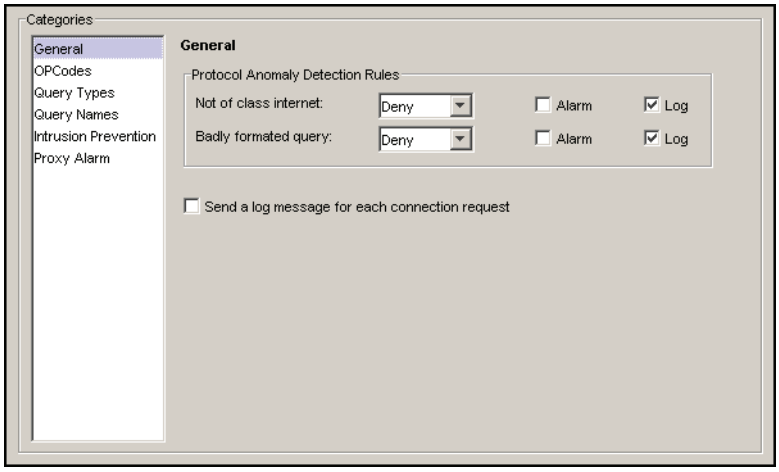
4 Select the **Properties** tab.

5 In the **Proxy** drop-down list, select to configure the NS-Outgoing or DNS-Incoming proxy action.

6 Click the View/Edit Proxy icon.
You can also clone an existing proxy action to create a new proxy action.

Configuring general settings for the DNS proxy

The general settings for the DNS Proxy include two protocol anomaly detection rules.



Not of class Internet

Select the action to do when the proxy examines DNS traffic that is not of the Internet (IN) class. The default action is to deny this traffic. We recommend that you do not change this default action. Use the **Alarm** check box to use an alarm for this event. Use the **Log** check box to write this event to the log file.

Badly formatted query

Select the action when the proxy examines DNS traffic that does not use the correct format. Use the **Alarm** check box to use an alarm for this event. Use the **Log check box** to write this event to the event log file.

Send a log message with summary information for each transaction

Select this check box to record a log message for each DNS connection request. Note that this creates a large number of log messages and traffic.

Configuring DNS OPcodes

DNS OPcodes are commands given to the DNS server that tell it to do some action, such as a query (Query), an inverse query (IQuery), or a server status request (STATUS). You can allow, deny, drop, or block specified DNS OPcodes.

1 From the **Categories** section, select **OPCodes**.

2 For the rules listed, select the **Enabled** check box to enable a rule. Clear the **Enabled** check box to disable a rule.

Note

If you use Active Directory and your Active Directory configuration requires dynamic updates, you must allow DNS OPcodes in your DNS-Incoming proxy action rules. This is a security risk, but can be necessary for Active Directory to operate correctly.

Adding a new OPcodes rule

1 Click **Add**.
The New OPCodes Rule dialog box appears.

2 Type a name for the rule.
Rules can have no more than 31 characters.

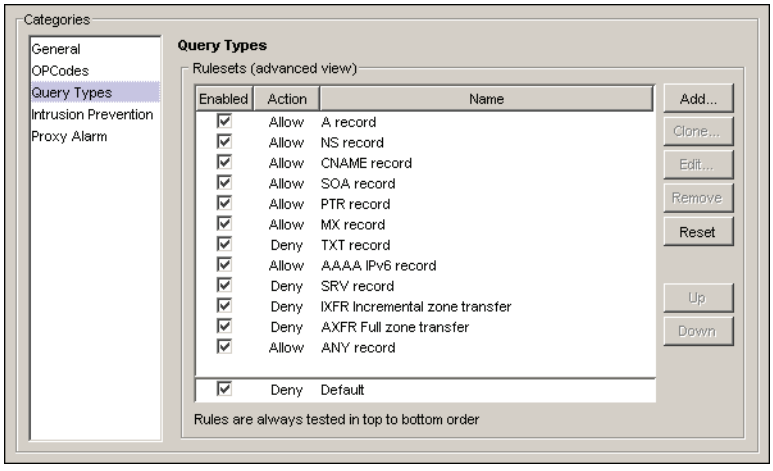
3 DNS OPcodes have an integer value. Use the arrows to set the OPCode value.
For more information on the integer values of DNS OPcodes, see RFC 1035.

4 Set an action for the rule and configure to send an alarm or enter the event in the log file. For more information, see "Adding rules" on page 80.

Configuring DNS query types

A DNS query type can configure a resource record by type (such as a CNAME or TXT record) or a custom type of query operation (such as an AXFR Full zone transfer). You can allow, deny, drop, or block specified DNS query types.

1 From the **Categories** section, select **Query Types**.



2 To enable a rule, select the **Enabled** check box adjacent to the action and name of the rule.

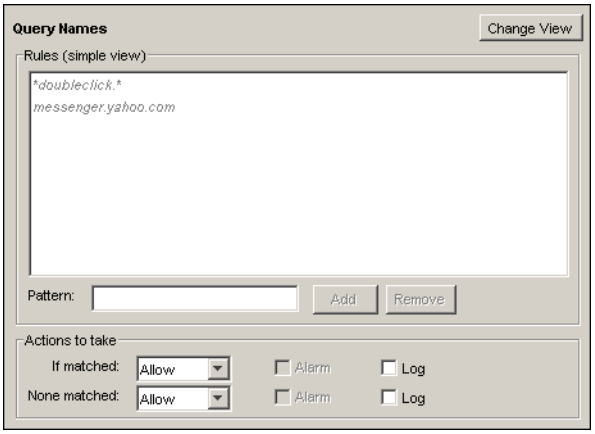
Adding a new query types rule

1 To add a new query types rule, click **Add**.
The New Query Types Rule dialog box appears.
2 Type a name for the rule.
Rules can have no more than 31 characters.
3 DNS query types have a resource record (RR) value. Use the arrows to set the value.
For more information on the values of DNS query types, see RFC 1035.
4 Set an action for the rule and configure to send an alarm or enter the event in the log file. For more information, see "Defining Rules" on page 161.

Configuring DNS query names

A DNS query name refers to a specified DNS domain name, shown as a fully qualified domain name (FQDN).

1 From the **Categories** section, select **Query Names**.



2 To add more names, do the steps used to create rules. For more information, see "Defining Rules" on page 161.

Enabling intrusion prevention for DNS

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Configuring DNS proxy alarms

Use these settings to set criteria for a notification event:

1 From the **Categories** section, select **Proxy Alarm**.
2 Do the procedure in "Using dialog boxes for alarms, log messages, and notification" on page 164.

Configuring the TCP Proxy

Transmission Control Protocol (TCP) is the primary protocol in TCP/IP networks. The IP protocol controls packets while TCP enables hosts to start connections and to send and receive data. A TCP proxy monitors TCP handshaking to see if a TCP session is legitimate.

Configuring general settings for the TCP proxy

HTTP proxy action

Select the HTTP proxy action to use for TCP connections. The TCP proxy applies the HTTP proxy ruleset to all traffic that it identifies as HTTP traffic.

Send a log message with summary information for each transaction

Select this check box to record a log message for all TCP connection requests. This feature creates a large number of log messages and traffic.

Enabling intrusion prevention for TCP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

CHAPTER 14

Generating Reports of Network Activity

Historical Reports is a tool that makes summaries and reports of the Firebox® log file. You can use these reports to learn about Internet use. You also can measure bandwidth and see which users and software applications use the most bandwidth. Historical Reports creates reports from the log files that are recorded on the WatchGuard® Log Server.

With the advanced features of Historical Reports, you can:

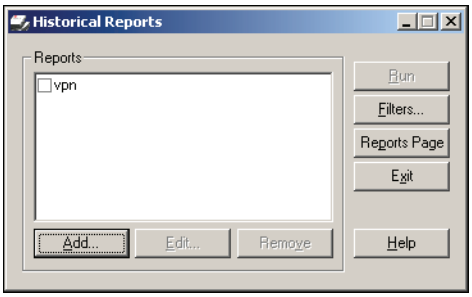
- Set a specified time period for a report.
- Customize the report with data filters.
- Consolidate different log files to create a report for a group of Fireboxes.
- Show the report data in different formats.

Creating and Editing Reports

When you make a report, you configure a group of settings that is used to create a report on a schedule that you select. This section shows you how to create, edit, and delete reports, and how to create a backup file of your report settings.

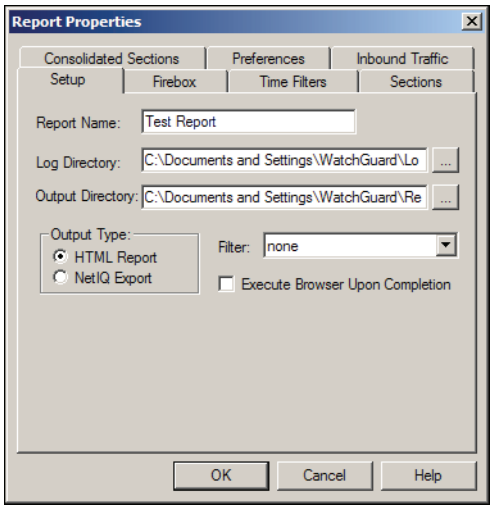
Starting Historical Reports

From the **Device Status** tab, click the Historical Reports icon.



Starting a new report

1 From Historical Reports, click **Add**.
The Report Properties dialog box appears.



2 Type the report name.
The report name appears in Historical Reports and in the name of the output file.

3 Use the text box in the **Log Directory** to give the location of the log files.
The default location for the log files is the path: My Documents\My WatchGuard\Shared WatchGuard\Logs.

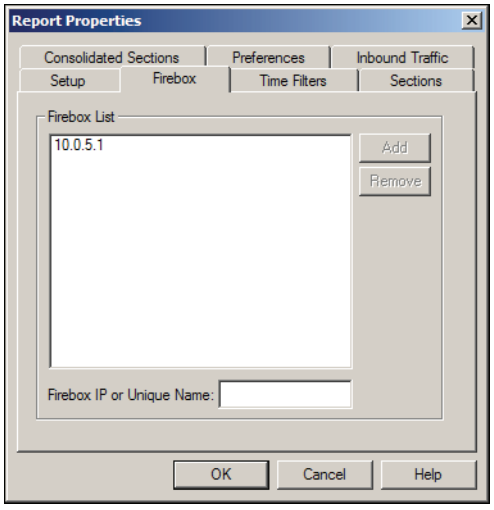
4 Use the text box in the **Output Directory** to give the location of the output files.
The default location for the output files is My Documents\My WatchGuard\Shared WatchGuard\reports.

5 To select the output type, click **HTML Report** or **NetIQ Export**.
For more information on output types, refer to "Exporting Reports" on page 190.

6 Select the filter.
For more information on the filters, refer to "Using Report Filters" on page 191.

7 To see the first page when you use the HTML output, select the **Execute Browser Upon Completion** check box.

8 Click the **Firebox** tab.



9 Type the Firebox® IP address or host name. Click **Add**.
When you type the IP addresses, type all the numbers and the periods. Do not use the TAB or the arrow key. When you create a report with consolidated sections, you must use only WFS Fireboxes or Fireboxes using Fireware®. If you use the two Firebox versions in a report the results are not correct.

10 Use the other tabs to set the report preferences. You can find information about this in subsequent sections of this chapter.

11 Complete the report configuration. Click **OK**.
The name of the report appears in the list of the reports.

Editing an existing report

You can change the definition of a report.

1 From Historical Reports, select the report to change. Click **Edit**.
The Report Properties dialog box appears.

2 Change the report definition.
To see the function of an item, right-click it, and then click What's This?.

Deleting a report

You can remove a report from the list of available reports.

From Historical Reports, select the report to change. Click **Remove**. This removes the <report name>.`rep` file from the `report-defs` directory.

Viewing the reports list

To see all the reports, click **Reports Page**. The reports appear in your default browser. You can move through all the reports in the list.

Backing up report definition files

Report definition files contain the settings for the reports you create. It is a good idea to create regular, frequent backup files of your report definition files. This can save you time later if you want to move your Log Server to a different computer. To create a backup file of your report definitions, copy the contents of the \Documents and Settings\WatchGuard\report-defs folder to an archive file. Keep it in a safe place.

Setting Report Properties

You use the **Report Properties** dialog box to configure many properties of reports. To see this dialog box:

- Select a report in Historical Reports and click **Edit**.

or

- In Historical Reports, click **Add**.

Specifying a report time interval

When you create a report, the report includes data from the full log file, unless you change the time interval. On the **Time Filters** dialog box, use the drop-down list to select a time interval, for example

"yesterday" or "today." You also can manually configure the start and end time. Thus the report uses only the specified time interval:

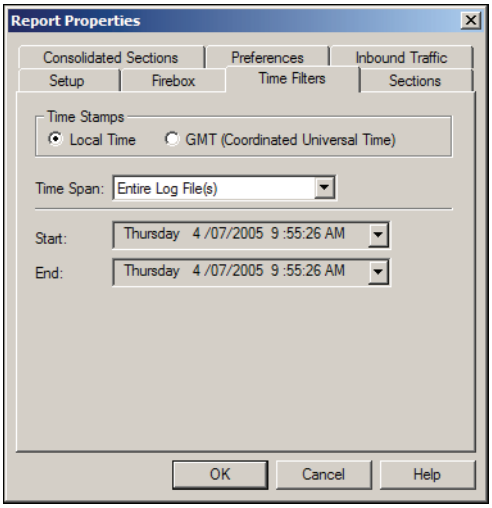
1 In the **Report Properties** dialog box, click the **Time Filters** tab.

2 Select the time-stamp to appear on your report: **Local Time** or **GMT**.

3 From the **Time Span** drop-down list, select the time interval for the report.

4 If you did not select **Specify Time Filters** in the **Time Span** drop-down list, click **OK**.

If you did select **Specify Time Filters**, click the **Start** and the **End** drop-down lists and select a start and an end time. Click **OK.**



Specifying report sections

You can select the information to show in the report using the **Sections** tab on the **Report Properties** dialog box.

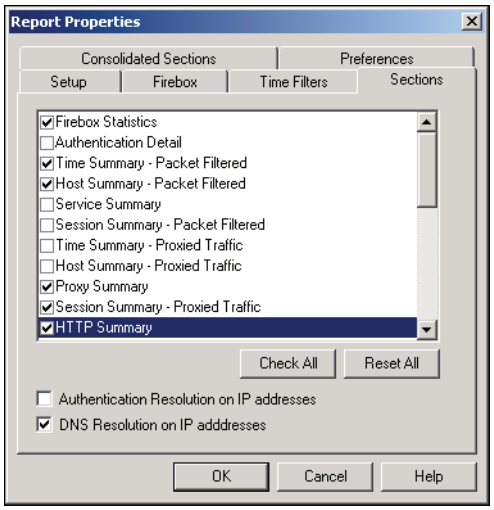
1 From Historical Reports, click the **Sections** tab.

2 Select the check boxes for the sections to include in the report.
To see the contents of each section, refer to the "Report Sections and Consolidated Sections" on page 193.

3 (Optional) To include the authentication names for the IP addresses of Firebox® authenticated users, select the **Authentication Resolution on IP addresses** check box.
You must have user authentication enabled to create reports with resolution from IP address to user name. More time is necessary to create a report with resolution enabled.

4 (Optional) To include DNS names for IP addresses, select the **DNS Resolution on IP addresses** check box.

This information is included only for IP addresses for which DNS information can be resolved from the Firebox.



Consolidating report sections

In the **Sections** tab you can select which information to include in a report. You can get:

- A vertical look at data, on each of a group of Fireboxes
- A horizontal or cumulative look at data, put together for a group of Firebox®devices.

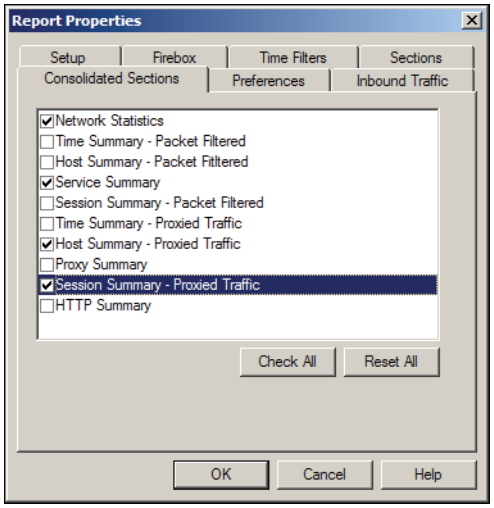
To consolidate report sections:

1 In the **Report Properties** dialog box, select the **Consolidated Sections** tab.

The tab has a list of report sections that you can put together. For short notes on the contents of these sections, refer to "Report Sections and Consolidated Sections" at the end of this chapter.

2 Select the check boxes adjacent to the sections to include in the report. Clear the check boxes for the sections to not include.

3 Click **OK.**



Setting report properties

Reports can have Summary sections or Detail sections. You can control the display of each section independently to best show the information that is important to you. A report summary section shows text and graphs that contain user-defined information.

To set the report properties:

1 From the **Report Properties** dialog box, select the **Preferences** tab.

2 Type the number of data points (items) to show as a graph in the report.
As an example, if you have 45 hosts, graph the top 10 and list the remaining hosts as "other". The default number is 10.

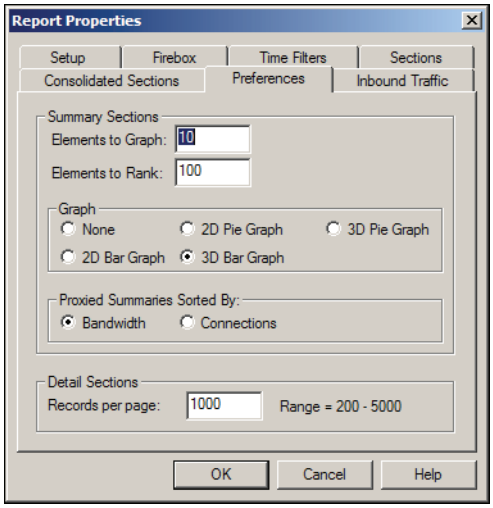
3 Type the number of items to put in the table.
The default number is 100.

4 Select the type of graph to use in the report.

5 Select how to sort the proxied summary: by bandwidth or by connections.

6 Type the number of records to show on each page of the detail sections.
The default number is 1,000 records.

7 Click **OK**.



Viewing network interface relationships

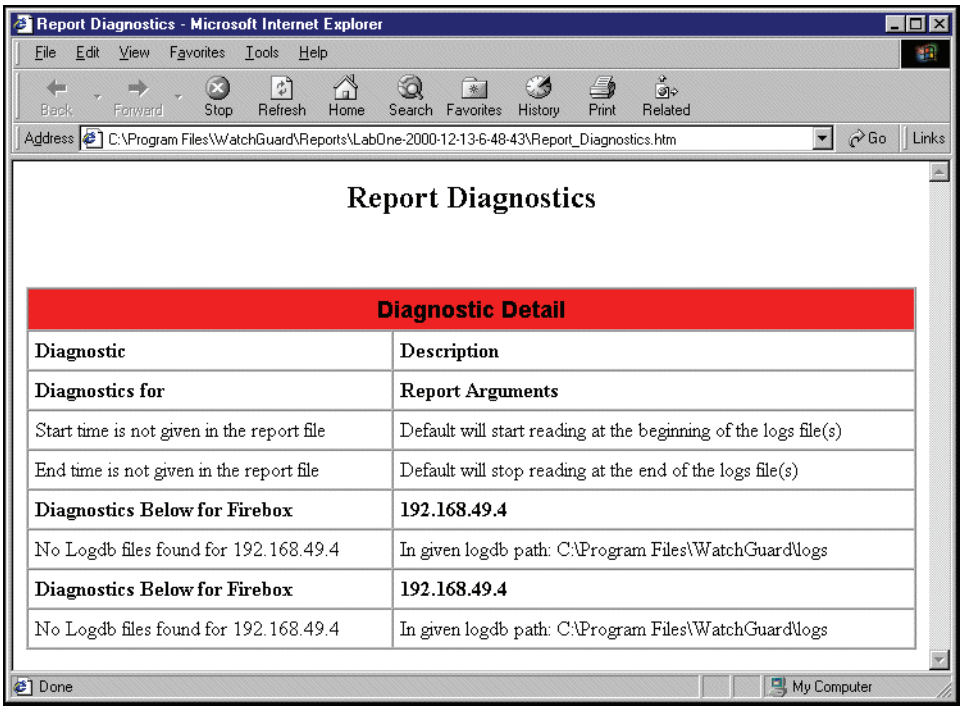
On the **Inbound Traffic** tab, you see all possible network interface relationships that the Firebox considers to be incoming. For example, traffic that comes from the optional network to the trusted network is considered incoming traffic. If you want to remove a relationship from the list, select it and click **Remove**. You also can add your own source and destination pair to the list. Click **Add** and type the new source and destination you want to set as incoming.

Exporting Reports

You can export a report to two formats: HTML and NetIQ. You can find all reports in the path My Documents\My WatchGuard\Shared WatchGuard\reports\<export file>. In the Reports directory are the subdirectories with the name and the time of each report.

Exporting reports to HTML format

If you select **HTML Report** from the **Setup** tab on the **Report Properties** dialog box, the report output is in HTML. You can go to each report section through a JavaScript menu. For this, you must enable JavaScript on the browser. The figure below shows how the report can appear in the browser.


Report Diagnostics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Print Related
Address C:\Program Files\WatchGuard\Reports\LabOne-2000-12-13-6-48-43\Report_Diagnostics.htm
Go Links
Report Diagnostics
Diagnostic Detail
Diagnostic
Description
Diagnostics for
Report Arguments
Start time is not given in the report file
Default will start reading at the beginning of the logs file(s)
End time is not given in the report file
Default will stop reading at the end of the logs file(s)
Diagnostics Below for Firebox
192.168.49.4
No Logdb files found for 192.168.49.4
In given logdb path: C:\Program Files\WatchGuard\logs
Diagnostics Below for Firebox
192.168.49.4
No Logdb files found for 192.168.49.4
In given logdb path: C:\Program Files\WatchGuard\logs
Done
My Computer

Exporting reports to NetIQ format

NetIQ supplies system and security management solutions, including full reports about how the Internet is used by an organization, but measures data differently than WatchGuard® Historical Reports. To calculate Internet use report data, Historical Reports counts the number of HTTP protocol transactions. NetIQ calculates the number of URL requests.

Note

The WatchGuard HTTP proxy logging must be set to ON to supply NetIQ with the information that is necessary.

You can find the report in:
My Documents\My WatchGuard\Shared WatchGuard\reports

Using Report Filters

A report includes data from the full log file unless you create and use report filters. You can use a report filter to show only data about specified hosts, services, or users. A filter can be one of two types:

Include

To make a report that includes records with the properties set in the **Host**, the **Service**, or the **User Report Filters** tabs.

Exclude
To make a report that does not include records with the properties set in the **Host**, the **Service**, or the **User Report Filters** tabs.

You can set a filter to Include or Exclude data in a report with three properties:

Host
Host IP address

Port
Service name or port number

User
Authenticated user name

Creating a new report filter

Use Historical Reports to make a new report filter. You can find the filters in the WatchGuard® installation directory, in the subdirectory `report-defs` with the file extension `.ftr`.

1 From Historical Reports, click **Filters**.

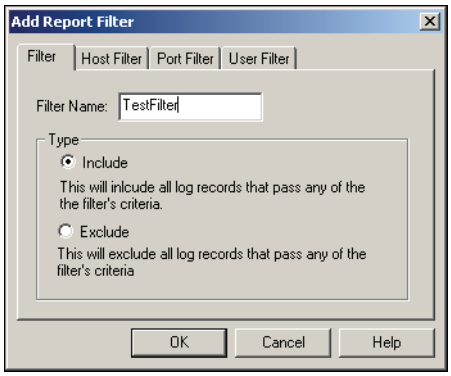
1 Click **Add**.

2 Type the name of the filter. This name appears in the **Filter** drop-down list on the **Report Properties Setup** tab.

3 Select the filter type.
As an example, if you have 45 hosts, graph the top 10 and list the remaining hosts as "other." For a description of include and exclude, see above.

4 Complete the **Filter** tabs.
To see the function of each item, right-click it, and then click What's This?.

5 When finished, click **OK**.
The name of the filter appears in the list of the filters. The Filter Name.ftr file is in My Documents\My WatchGuard\Shared WatchGuard\report-defs.



Editing a report filter

You can change the properties of a filter. From the **Filters** dialog box in Historical Reports:

1 Select the filter to change. Click **Edit**.
The Report Filter dialog box appears.

2 Change the filter properties.
To see the function of each property, right-click it, and then click What's This?.

Deleting a report filter

To remove a filter from the list of filters, select the filter. Click **Delete**. This removes the `.ftr` file from the `\report-defs` directory.

Applying a report filter

Each report can use only one filter. To apply a filter, open the report properties.

1 From Historical Reports, select the report to apply a filter to. Click **Edit**.

2 Use the **Filter** drop-down list to select a filter.
Only if you make a filter in the Filters dialog box will it appear in the drop-down list. For more information, see "Creating a new report filter" on page 192.

3 Click **OK**.
Save the new report to the ReportName.rep file in the report-defs directory. When you make the report, the filter is applied.

Running Reports

You can create one or more reports with Historical Report.

1 From Historical Reports, select the check box adjacent to each report that is necessary.

2 Click **Run**.

Note

If the **Send a log message with summary information for each transaction** check box in your HTTP proxy action is not selected, you do not see detailed information about HTTP proxied connections in your reports.

Report Sections and Consolidated Sections

You can use Historical Reports to create a report with one or more sections. Each section includes a different type of information or network traffic. You can put together specified sections to create a summary. You can then create a report on the event log messages of a group of Firebox®devices.

Report sections

There are two basic types of Report sections:

- **Summary —** The sections that rank data by bandwidth or connections.
- **Detailed —** The sections that show all traffic and events with no summary graph or rank.

A list of the different types of the report sections and the consolidated sections is shown below:

Firebox Statistics
A summary of the statistics on one or more log files for one Firebox.

Authentication Detail
A list of authenticated users in the sequence of connection time. The text boxes include:
- Authenticated user
- Host

- Start date and start time of the authenticated session
- End time of the authenticated session
- Length of the session

Time Summary — Packet Filtered

A table, and an optional graph, of all the accepted connections that is divided by user-defined intervals and time. The default time interval is each day, but you can select a different time interval.

Host Summary — Packet Filtered

A table, and an optional graph, of the internal and the external hosts that send packet-filtered traffic through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Service Summary

A table, and an optional graph, of the traffic for each service in the sequence of the connection count.

Session Summary — Packet Filtered

A table, and an optional graph, of the top incoming and outgoing sessions. The sessions show in sequence of the volume of bytes or the number of connections. The format of the session is: client > server: service. Historical Reports tries to look up the server port with a table to show the service name. If this does not work, Historical Reports shows the port number.

Time Summary — Proxied Traffic

A table, and an optional graph, of all the accepted connections divided by user-defined intervals and in the sequence of the time. The default time interval is each day, but you can select a different time interval.

Host Summary — Proxied Traffic

A table, and an optional graph, of the internal and the external hosts that send traffic with a proxy through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Proxy Summary

The proxies in the sequence of bandwidth or connections.

Session Summary — Proxied Traffic

A table, and an optional graph, of the top incoming sessions and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. The service shows in all uppercase letters.

HTTP Summary

Tables, and an optional graph, of the top external domains and hosts that users connect to through the HTTP proxy. The domains and the hosts show in the sequence of the byte count or number of connections.

HTTP Detail

Tables for incoming and outgoing HTTP traffic in the sequence of the time stamp. The fields are Date, Time, Client, URL Request, and Bytes Transferred.

SMTP Summary

A table, and an optional graph, of the top incoming and outgoing e-mail addresses in the sequence of the volume of bytes or the number of connections.

SMTP Detail

A table of the incoming and the outgoing SMTP proxy traffic in the sequence of the time stamp. The fields are: Date, Time, Sender, Recipient(s), and Bytes Transferred.

FTP Detail

Tables for incoming and outgoing FTP traffic, in the sequence of the time stamp. The fields are Date, Time, Client, Server, FTP Request, and Bandwidth.

Denied Outgoing Packet Detail

A list of denied outgoing packets, in the sequence of the time. The fields are: Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Incoming Packet Detail

A list of denied incoming packets, in the sequence of the time. The fields are Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Packet Summary

In this section there are different tables. Each table shows the data on the host that denied packets. The data has the time of the first and the last try, the type, the server, the port, the protocol, and the number of tries. If there is only one try, the last field has no data.

Denied Service Detail

A list of events in which a user was denied use of a service. This list includes Incoming and Outgoing requests.

WebBlocker Detail

A list of URLs denied because of WebBlocker™, in the sequence of time. The fields are Date, Time, User, Web Site, Type, and Category.

Denied Authentication Detail

A list of each denied authentication, in the sequence of the time. The fields are Date, Time, Host, and User.

IPS Blocked Sites

A list of the IPS blocked sites.

Alarms

Available for Fireware® users only, this report shows all device alarms and the problem found with each alarm.

AV Summary

A summary of Gateway AntiVirus for E-mail actions. The fields include sender, virus detail, if the virus was cleaned, and attachment size of the e-mail. This section is available to Fireware users who subscribe to the antivirus service.

AV Detail

A list of the source, sender, and virus detail for Gateway AntiVirus for E-mail actions. This section is available to Fireware users who subscribe to the antivirus service.

IPS Summary

A summary of Intrusion Prevention Service (IPS) actions, showing percentage traffic type, source IP address, and signature category. This section is available to Fireware users who subscribe to the IPS service.

IPS Detail

A list of all Intrusion Prevention Service actions, including source, protocol, and signature detail. This section is available to Fireware users who subscribe to the IPS service.

Consolidated sections

Network Statistics
A summary of the statistics on one or more log files for all the Fireboxes that are monitored.

Time Summary — Packet Filtered
A table, and an optional graph, of all accepted connections divided by user-defined intervals and in the sequence of time. The default time interval is each day, but you can select a different time interval.

Host Summary — Packet Filtered
A table, and an optional graph, of the internal and external hosts that send packet-filtered traffic through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Service Summary
A table, and an optional graph, of the traffic for all services in the sequence of the connection count.

Session Summary — Packet Filtered
A table, and an optional graph, of the top incoming and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. Historical Reports tries to look up the server port with a table to show the service name. If this does not work, Historical Reports shows the port number.

Time Summary — Proxied Traffic
A table, and an optional graph, of all the accepted connections divided by user-defined intervals and in the sequence of the time. The default time interval is each day, but you can select a different time interval.

Host Summary — Proxied Traffic
A table, and an optional graph, of the internal and external hosts that send traffic with a proxy through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Proxy Summary
The proxies in the sequence of bandwidth or connections.

Session Summary — Proxied Traffic
A table, and an optional graph, of the top incoming sessions and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. The service shows in all uppercase letters.

HTTP Summary
Tables, and an optional graph, of the top external domains and hosts that users connect to through the HTTP proxy. The domains and the hosts show in the sequence of the byte count or the number of connections.

CHAPTER 15

Management Server Setup and Administration

The WatchGuard® Management Server manages the VPN tunnels of a distributed enterprise from one easy-to-use management interface. The Management Server also allows you to centrally manage multiple Firebox® X Edge devices. After you complete the setup procedures in this chapter, you can use the WatchGuard® Management Server to configure and manage a Firebox device that is connected to the Management Server. You can open the correct tools from the Management Server device page to manage Firebox X Core, Firebox X Peak, Firebox III, Firebox X Edge, and SOHO 6 devices. For more information, see the subsequent chapter.

You can use the WatchGuard Management Server to configure and manage multiple Firebox X Edge devices. For more information, see the "Managing the Firebox X Edge and Firebox SOHO" chapter.

You can install the Management Server on your management station during installation. Or, you can use the same installation procedure to install the Management Server on a different computer that uses the Windows operating system. We recommend that you install the Management Server software on a computer with a static IP address that is behind a Firebox with a static external IP address. Otherwise, the Management Server may not operate correctly.

WatchGuard Management Server Passphrases

The WatchGuard® Management Server uses a number of passwords to protect sensitive information on its hard disk and to secure data with client systems. After you install the WatchGuard Management Server software, you must use the Configuration Wizard to configure the Management Server. This wizard prompts for these passphrases:

- Master encryption key
- Management Server passphrase

The Management Server passphrase and other automatically created passphrases are kept in a passphrase file.

Master encryption key

The first passphrase that you set with the Configuration Wizard is the master encryption key. This passphrase protects all passphrases in the passphrase file.

The master encryption key is used to encrypt all other passphrases that are on the hard drive of the Management Server. This prevents a person with access to the hard drive or its archived contents from getting the passphrases and using them to get access to other sensitive data on the hard drive.

Select and secure the master encryption key carefully. Make sure that the master encryption key and the Management Server passphrase are not the same.

You use the master encryption key when you:

- Migrate the Management Server data to a new system
- Restore a lost or corrupt master key file
- Change the master encryption key

The master encryption key is not used frequently. We recommend that you write it down and lock it in a secure location.

Management Server passphrase

The second passphrase that the Configuration Wizard prompts for is the Management Server passphrase. This passphrase is used frequently by the administrator. You use this passphrase to connect to the Management Server in WatchGuard System Manager.

Password and key files

The Management Server passphrase and all the automatically created passphrases are kept in a passphrase file. The passphrase data in this file is protected by the master encryption key. The master encryption key is not kept on the hard drive. An encryption key is created from the master encryption key.

The default locations for the password file and encryption key are:

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini
- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

Note that these files are used by the Management Server software and must not be modified directly by an administrator.

Microsoft SysKey utility

The password file is protected by the master key. This key is protected by an encryption key, which is protected by the Windows system key.

Windows operating systems use a system key to protect the Security Accounts Management (SAM) database. This is a database of the Windows accounts and passwords on the computer. By default, the system key data is hidden in the registry. The system is protected, and the system key is created from the registry during the startup procedure. If you want a more secure system, you can remove the system key data from the registry so that this sensitive data is not on the system at all.

You can use the SysKey utility to:

- Move the system key to a floppy disk
- Make the administrator type a password at start time
- Move the system key from the floppy disk to the system

If you move the startup key to a floppy disk, then that disk must be inserted in the drive for the system to start. If you make the administrator type a startup password, the administrator must type in the password each time the system starts.

To configure SysKey options, click **Start > Run**, type **syskey**, and click **OK**.

Setting Up the Management Server

The Management Server Setup wizard creates a new Management Server on your workstation. If you used earlier versions of WatchGuard® System Manager and VPN Manager, you can also use the wizard to migrate a DVCP Server that is installed on a Firebox® to a new Management Server on a workstation. To move a Management Server off a Firebox, see the *WFS to Fireware Migration Guide*.

We recommend that you install the Management Server software on a computer with a static IP address that is behind a Firebox with a static external IP address. Otherwise, the Management Server may not operate correctly.

This procedure shows the steps you must use to successfully set up a new Management Server. Use this procedure if you do not have a Management Server at this time.

1 Right-click the Management Server icon in the WatchGuard toolbar on the Windows taskbar
You do not see this icon if you have not installed the Management Server.

2 Select **Start Service**.

3 The Management Server Setup wizard starts. Click **Next**.

4 A master encryption key is necessary to control access to the WatchGuard management station. Type a passphrase that has a minimum of eight characters and then type it again to confirm. Click **Next**.
Make sure you keep this passphrase in a safe place.

5 Type the Management Server passphrase to use when you configure and monitor the WatchGuard Management Server. Use a passphrase that has a minimum of eight characters and then type it again to confirm. Click **Next**.

6 Type the IP address and passphrases for your gateway Firebox. The gateway Firebox protects the Management Server from the Internet. When you add an IP address, the wizard does three things:
- The wizard uses this IP address to configure the gateway Firebox to allow connections to the Management Server. If you do not type an IP address here, you must configure any firewall between the Management Server and the Internet to allow connections to the Management Server on TCP ports 4110, 4112, and 4113.
- If you have an earlier version of WatchGuard System Manager, and have a Firebox configured as a DVCP server, the wizard gets the DVCP server information from the gateway Firebox and moves these settings to your Management Server. See the *Migration Guide* for more information.
- The wizard sets the IP address for the Certificate Revocation List. The devices you add as managed clients use this IP address to connect to the Management Server. This IP address must be the public IP address your Management Server shows to the Internet. If you do not type an IP address here, the wizard uses the current IP address on your Management Server computer for the CRL IP address. If this is not the IP address your computers shows to the Internet because your computer is behind a device that does Network Address Translation (NAT), you must edit the CRL and type the public IP address your Management Server uses. For more information, see “Changing the Management Server Configuration” on page 200.

7 Type the license key for the Management Server. Click **Next**.
For more information on Management Server license keys, see this Advanced FAQ:
https://www.watchguard.com/support/AdvancedFaqs/wsm8_srvrkey.asp

8 Type the name of your organization. Click **Next**.
This name is used for the Certificate Authority on the Management Server.

9 An information screen that shows the information for your server appears. Click **Next**.
The wizard configures the server.

10 Click **Finish**.

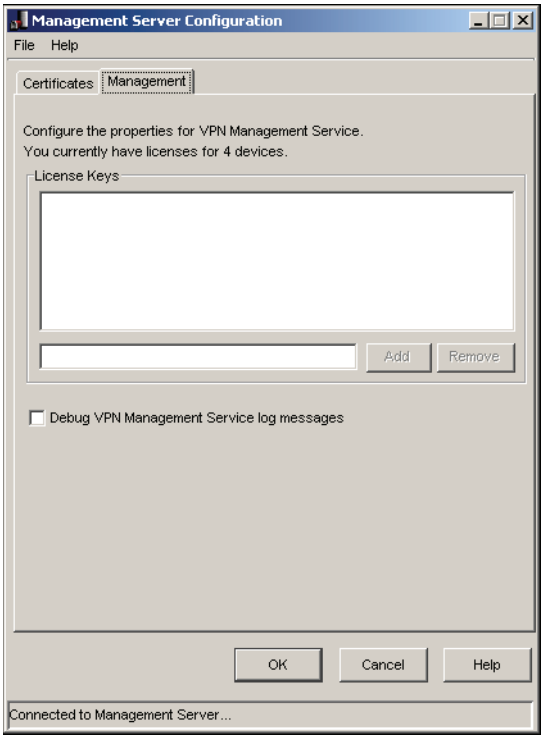
Note

When an interface whose IP address is bound to the Management Server goes down and then restarts, we recommend that you restart the Management Server.

Changing the Management Server Configuration

The Management Server Setup Wizard configures your Management Server. It is not usually necessary to change the properties of your Management Server configuration after you use the wizard. If you must change the Management Server configuration, you can access the configuration properties on the Management Server itself.

From the computer configured as a Management Server, right-click the Management Server icon in the WatchGuard® toolbar and select **Configure**. The **Management Server Configuration** dialog box appears.



Adding or removing a Management Server license

To add a Management Server license, click the **Management** tab. Type or paste the Management Server license key into the field, and click **Add**.

To remove a Management Server license, click the **Management** tab. Select the license to remove, and click **Remove**.

Click **OK** when you complete the configuration.

For more information on Management Server license keys, see this Advanced FAQ:
https://www.watchguard.com/support/AdvancedFaqs/wsm8_srvrkey.asp

Recording diagnostic log messages for the Management Server

To have the Management Server send diagnostic log messages to the Windows Event Viewer, click the Management tab. Select the **Debug VPN Management Service log messages** check box.

To see the diagnostic log messages, open the Windows Event Viewer. From the Windows desktop, select **Start > Run**. Type `eventvwr`. Look in the Application section of the Event Viewer to see the log messages.

Configuring the Certificate Authority

You can configure the Certificate Authority (CA) on the WatchGuard Management Server. Use the Certificate Authority to:

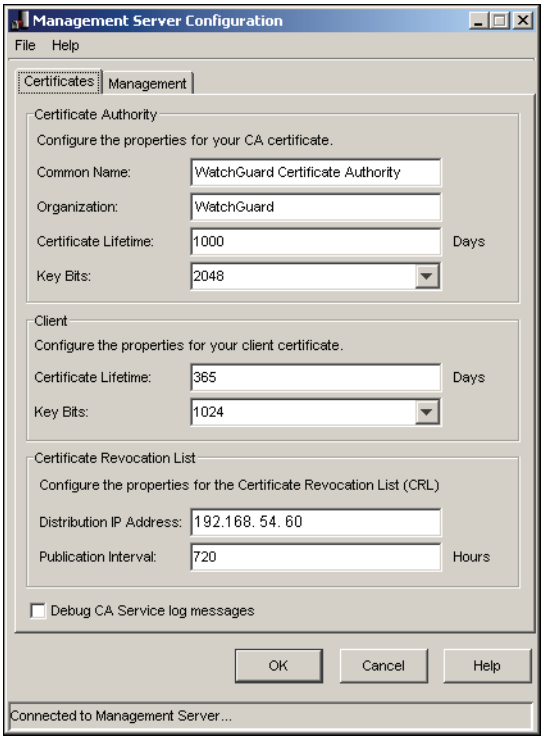
- Configure the properties of the CA certificate
- Configure the properties of the client certificate
- Configure properties for the Certificate Revocation List (CRL)
- Write CA Service diagnostic log messages to the Windows Event Viewer

Configuring properties for the CA certificate

Usually, Firebox administrators do not change the properties of the CA certificate. If you must change these settings:

1 From the computer configured as a Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**.

2 Click the **Certificates** tab.


Management Server Configuration
File Help
Certificates Management
Certificate Authority
Configure the properties for your CA certificate.
Common Name: WatchGuard Certificate Authority
Organization: WatchGuard
Certificate Lifetime: 1000 Days
Key Bits: 2048
Client
Configure the properties for your client certificate.
Certificate Lifetime: 365 Days
Key Bits: 1024
Certificate Revocation List
Configure the properties for the Certificate Revocation List (CRL)
Distribution IP Address: 192.168. 54. 60
Publication Interval: 720 Hours
Debug CA Service log messages
OK Cancel Help
Connected to Management Server...

3 In the **Common Name** text box, type the name you want to appear in the CA certificate.

4 In the **Organization** text box, type an organization name for the CA certificate.

5 In the **Certificate Lifetime** text box, type the number of days after which the CA certificate will expire.
A longer certificate lifetime could give an attacker more time to attack it.

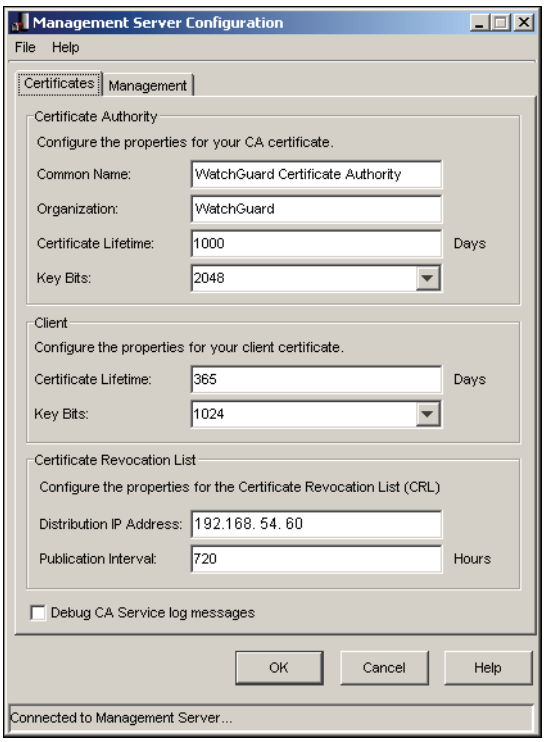
6 From the **Key Bits** drop-down list, select the strength to apply to the certificate.
The higher the number in the Key Bits setting, the stronger the cryptography that protects the key.

7 Click **OK** when you complete the configuration.

Configuring properties for client certificates

1 From the computer defined as a Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**.

2 Click the **Certificates** tab.


Management Server Configuration
File Help
Certificates Management
Certificate Authority
Configure the properties for your CA certificate.
Common Name: WatchGuard Certificate Authority
Organization: WatchGuard
Certificate Lifetime: 1000 Days
Key Bits: 2048
Client
Configure the properties for your client certificate.
Certificate Lifetime: 365 Days
Key Bits: 1024
Certificate Revocation List
Configure the properties for the Certificate Revocation List (CRL)
Distribution IP Address: 192.168. 54. 60
Publication Interval: 720 Hours
Debug CA Service log messages
OK Cancel Help
Connected to Management Server...

3 In the **Certificate Lifetime** text box, type the number of days after which the client certificate will expire.
A longer certificate lifetime could give an attacker more time to attack it.

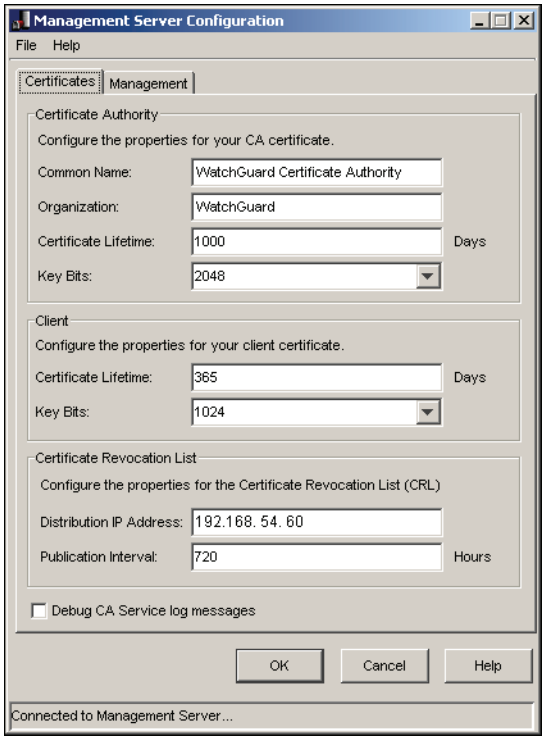
4 From the **Key Bits** drop-down list, select the strength to apply to the certificate.
The higher the number in the Key Bits setting, the stronger the cryptography that protects the key.

5 Click **OK** when you complete the configuration.

Configuring properties for the Certificate Revocation List (CRL)

1 From the computer defined as a Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**.

2 Click the **Certificates** tab.


Management Server Configuration
File Help
Certificates Management
Certificate Authority
Configure the properties for your CA certificate.
Common Name: WatchGuard Certificate Authority
Organization: WatchGuard
Certificate Lifetime: 1000 Days
Key Bits: 2048
Client
Configure the properties for your client certificate.
Certificate Lifetime: 365 Days
Key Bits: 1024
Certificate Revocation List
Configure the properties for the Certificate Revocation List (CRL)
Distribution IP Address: 192.168. 54. 60
Publication Interval: 720 Hours
Debug CA Service log messages
OK Cancel Help
Connected to Management Server...

3 Type the **Distribution IP Address** for the Certificate Revocation List (CRL).
By default, this is the address of the gateway Firebox. This is also the IP address the remote managed Firebox clients use to connect to the Management Server. If the external IP address of your Firebox changes, you must change this value.

4 Type the **Publication Interval** for the CRL in hours. This is the period after which the CRL is automatically published.
The default setting is zero (0), which means that the CRL is published every 720 hours (30 days). The CRL is also updated after a certificate is revoked.

5 Click **OK** when you complete the configuration.

Recording diagnostic log messages for the Certificate Authority service

To have the Management Server send diagnostic log messages to the Windows Event Viewer, click the **Certificates** tab. Select the **Debug CA Service log messages** check box. To see the log messages, open the Windows Event Viewer.

Backing up or Restoring the Management Server Configuration

The Management Server contains the configuration information for all managed Firebox® X Edge and VPN tunnels. It is a good idea to create regular and frequent backup files for the Management Server and keep them in a safe place. You can use this backup file to restore the Management Server in case of hardware failure. You can also use this backup file if you want to move the Management Server to a new

computer. To use the backup file after it is created, you must know the master encryption key. The master encryption key is set when you first configure the Management Server.

1 From your Windows toolbar, right-click the Management Server icon and select **Stop Service**.

2 From your Windows toolbar, right-click the Management Server icon and select **Backup/Restore**.
The Management Server Backup/Restore Wizard starts. Use the onscreen instructions to create a backup file or restore a Management Configuration from a backup file.

3 When the procedure is complete, right-click the Management Server icon on your Windows toolbar and select **Start Service**.

Moving the WatchGuard Management Server to a New Computer

To move the Management Server to a new computer, you must know the master encryption key. You must also make sure that the new Management Server is given the same IP address as the former Management Server.

1 Use the Management Server Backup/Restore Wizard to:
- Create a backup file of your current Management Server configuration.
- Install the Management Server software on the new Management Server.
- Use the WatchGuard® System Manager installation file and install the Management Server software.

2 Run the Restore wizard and select the backed up file.

3 From the Windows toolbar, right-click the Management Server icon and select **Start Service**.

CHAPTER 16

Using the Management Server

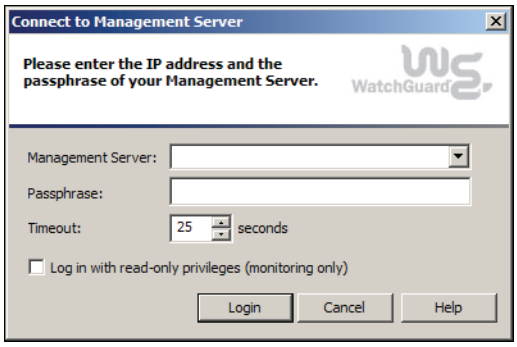
After you have set up and configured the Management Server, you can use it to manage VPN tunnels, and multiple Firebox® devices.

You can also use the Management Server to manage and configure Firebox X Edge devices. For more information, see the "Managing the Firebox X Edge and Firebox SOHO" chapter.

Connecting to a Management Server

1 Select **File > Connect to Server**.
or
Right-click anywhere in the Watchguard® System Manager window and select **Connect to > Server**.

or
Click the Connect to Server icon on the WatchGuard System Manager toolbar. The icon is shown at left.



2 From the **Management Server** drop-down list, select a server by its host name or IP address.
You can also type the IP address or host name if necessary.
When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow keys.

3 Type the passphrase for the Management Server.

4 If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that Watchguard System Manager listens for data from the Management Server before it sends a message that it cannot connect.

   If you have a slow network or Internet connection to the device, you can increase the time-out value. If you decrease the value it decreases the time you must wait for a time-out message if you try to connect to a Management Server that is not available.

5 If you are using the server only to monitor traffic, select the **Monitoring Only** check box. Do not select this check box if you must configure the server or its managed devices.

6 Click **OK**.
   The server appears in the WatchGuard System Manager window.

Note

In some previous versions of WatchGuard security products, the WatchGuard Management Server was called the DVCP Server.

Disconnecting from a Server

To disconnect, click on the Management Server name and select **File > Disconnect**. Or select the Management Server in the tree view and then click the Disconnect icon shown at left.

Managing Devices with the Management Server

To manage a Firebox with the Management Server, you must:

- Make sure the Firebox allows management connections from the Management Server
- For any Firebox that has a dynamic external IP address, manually enable the Firebox as a managed client
- Add the Firebox to the Management Server configuration.

The instructions you use to enable a Firebox as a managed Firebox client are different if you use different Firebox appliance software or a different Firebox model. The instructions can also be different if the managed Firebox client has a dynamic IP address. When you look at the sections below, make sure you find the information that matches your Firebox configuration.

Configuring a Firebox X Core or X Peak Running Fireware as a Managed Client

1 Open Policy Manager for the Firebox you want to enable as a managed client.

2 Double-click the **WatchGuard** policy to open it for editing.
   The Edit Policy Properties dialog box for the WatchGuard policy appears.

3 Make sure the **WatchGuard-Firebox-Mgmt connections are** drop-down list is set to **Allowed**.

4 Below the **From** dialog box, click **Add**. Click **Add Other**.

5 Make sure the **Choose Type** drop-down list is set to **Host IP**. In the **Value** field, type the IP address of the external interface of the gateway Firebox that protects the Management Server from the Internet.
   If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.

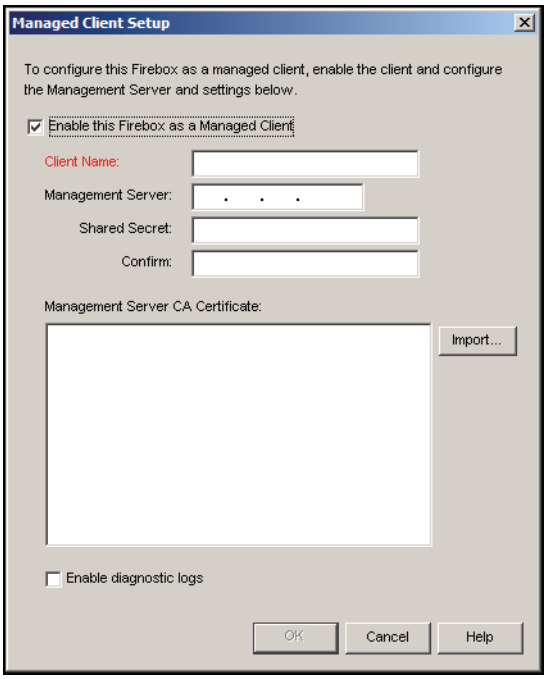
6 Click **OK**. Click **OK** again.

7 Make sure the **To** dialog box includes an entry of either **Firebox** or **Any**.

Note

If the Firebox you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Firebox to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Firebox as a managed Firebox client.
If the Firebox you want to manage has a dynamic IP address, go on to step 8.

8 From Policy Manager, select **VPN > Managed Client**.
The Managed Client Setup dialog box appears.



9 To set up a Firebox as a managed device, select the **Enable this Firebox as a Managed Client** check box.

10 In the **Client Name** box, type the name you want to give the Firebox when you add it to the Management Server configuration.
This name is case-sensitive and must match the name you use when you add the device to the Management Server configuration.

11 To enable the managed client to send log messages to the Log Server, select the **Enable diagnostic logs** check box. (We recommend this option only to perform troubleshooting.)

12 In the **Management Server** address box, type the IP address of the Management Server if it has a public IP address. Or, type the public IP address of the Firebox that protects the Management Server.
The Firebox protecting the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. The Firebox protecting the Management Server is configured to do this when you run the Management Server Setup Wizard.
If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the "Gateway Firebox" step in the wizard, configure the gateway Firebox to forward TCP ports 4110, 4112, and 4113 to the private IP address of the Management Server.

13 In the **Shared Secret** box, type the shared secret. Type it again to confirm.
The shared secret you type here must match the shared secret you type when you add the Firebox to the Management Server configuration.

14 Click the **Import** button and import the CA-Admin.pem file as your certificate.

15 Click **OK**.

When you save the configuration to the Firebox, the Firebox is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed Firebox client.

Configuring a Firebox III or Firebox X Core Running WFS as a Managed Client

1 Open Policy Manager for the Firebox you want to enable as a managed client.

2 Double-click the **WatchGuard** service to open it for editing.

The Edit Service Properties dialog box for the WatchGuard policy opens.

3 On the **Incoming** tab, make sure that incoming WatchGuard connections are set to **Enabled and Allowed**.

4 Below the **From** dialog box, click **Add**. Click **Add Other**.

5 Make sure the **Choose Type** drop-down list is set to **Host IP Address**. In the **Value** field, type the IP address of the external interface of the gateway Firebox that protects the Management Server from the Internet.

If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.

6 Click **OK**. Click **OK** again.

7 Make sure the **To** dialog box includes an entry of either **Firebox** or **Any**.

Note

If the Firebox you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Firebox to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Firebox as a managed Firebox client.

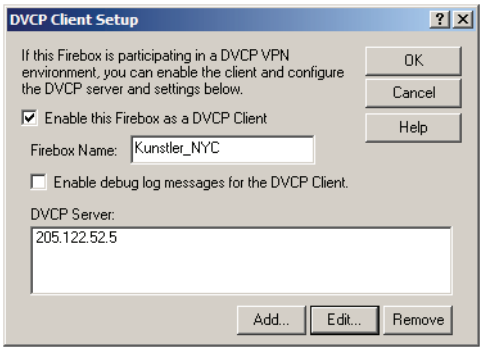
If the Firebox you want to manage has a dynamic IP address, go on to step 8.

8 From Policy Manager, select **Network > DVCP Client.**

9 Select the check box **Enable this Firebox as a DVCP Client**.

10 In the **Firebox Name** field, give the name of the Firebox.

The Firebox name is case-sensitive. The name you type here must match the name you type when you add this Firebox to the Management Server configuration.



11 To send log messages for the Managed Client, select the check box **Enable debug log messages for the DVCP Client**. (WatchGuard recommends this option only to do troubleshooting.)

12 Click **Add** to add the Management Server the Firebox connects to. In the **DVCP Server** address box, type the IP address of the Management Server if it has a public IP address. Or, type the public IP address of the Firebox that protects the Management Server. Type the **Shared Secret** to use to connect to the Firebox. The shared secret you type here must match the shared secret you type

when you add this device to the Management Server configuration.
A Firebox can be a client of only one Management Server.

The Firebox protecting the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. The Firebox protecting the Management Server is configured to do this when you run the Management Server Setup Wizard.
If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the "Gateway Firebox" step in the wizard, configure the gateway Firebox to forward TCP ports 4110, 4112, and 4113 to the private IP address of the Management Server.

13 Click **OK**.

When you save the configuration to the Firebox, the Firebox is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed Firebox client.

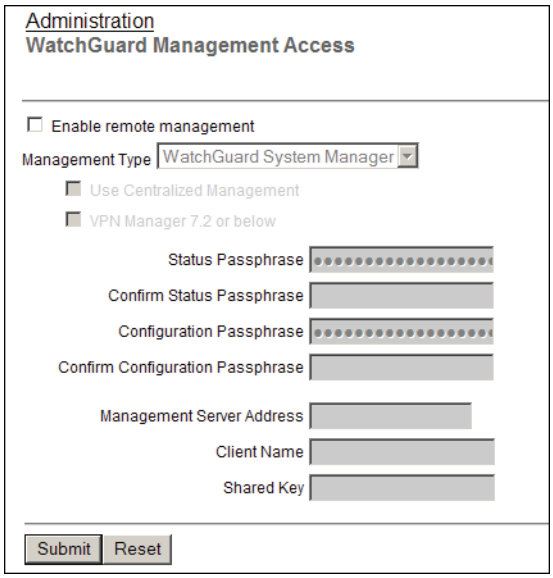
Configuring a Firebox X Edge as a Managed Client

1 To connect to the Firebox X Edge System Status page, type `https://` in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration > WSM Access**.

The WatchGuard Management Access page appears.



3 Select the **Enable remote management** check box.

4 From the **Management Type** drop-down list, select WatchGuard System Manager.

5 To put the Firebox X Edge into the control of WatchGuard System Manager centralized Edge management, click the **Use Centralized Management** check box. Do not select the **Use Centralized Management** check box if you are using WatchGuard System Manager only to manage VPN tunnels.

When the Firebox X Edge is under centralized management, access to the Firebox X Edge configuration pages is set to read-only. The only exception is access to the WSM Access configuration page. If you disable the remote management feature, you get read-write access to the Firebox X Edge configuration pages again.

6 Type a status passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.

7 Type a configuration passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.

These passphrases must match the passphrases you use when you add the device to the Management Server or the connection will fail.

Note

If the Firebox X Edge you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Edge to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Edge as a managed Firebox client.
If the Edge you want to manage has a dynamic IP address, go on to step 8.

8 In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox that protects the Management Server.
The Firebox that protects the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.

9 Type the **Client Name** to give your Edge to identify the Edge in the Management Server configuration.
This name is case-sensitive and must match the name you use for the Edge when you add it to the Management Server configuration.

10 Type the **Shared Key**.
The shared key is used to encrypt the connection between the Management Server and the Firebox X Edge. This shared key must be the same on the Edge and the Management Server. You must get the shared key from your Management Server administrator.

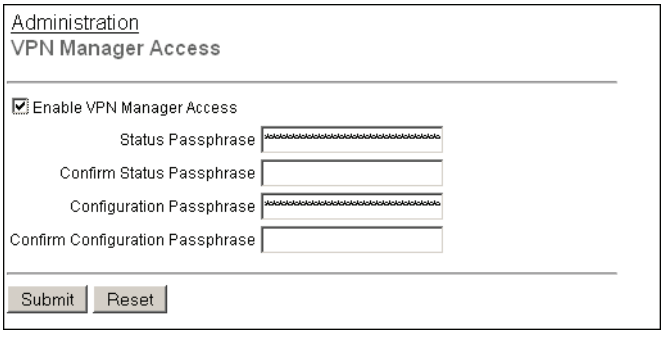
11 Click **Submit** to save this configuration to the Firebox X Edge.
When you save the configuration to the Edge, the Edge is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed Firebox client.

Configuring a Firebox SOHO 6 as a Managed Client

1 Start your web browser. Type the IP address of the SOHO 6.

2 If the SOHO 6 must have a login and passphrase, type the login and passphrase.

3 Below Administration, click **VPN Manager Access**.
The VPN Manager Access page appears.



4 In the left navigation pane below VPN, click **Managed VPN**. Select the **Enable VPN Manager Access** check box.

5 Type the status passphrase for VPN Manager access. Type the status passphrase again to confirm the passphrase.

6 Type the configuration passphrase for VPN Manager access. Type the configuration passphrase again to confirm the passphrase.

Note

If the Firebox SOHO you want to manage has a static IP address on its external interface, you can stop here. Click Submit to save your configuration to the SOHO. You can now add the device to your Management Server configuration. When you add this SOHO to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the SOHO as a managed Firebox client.
If the SOHO you want to manage has a dynamic IP address, go on to step 7.

7 Select the **Enable Managed VPN** check box.

8 From the **Configuration Mode** drop-down list, select **SOHO**.

9 In the **DVCP Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox that protects the Management Server.
The Firebox that protects the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.

10 Type the **Client Name** to give your Firebox SOHO.
This name is case-sensitive and must match the name you use for the Edge when you add it to the Management Server configuration.

11 Type the **Shared Key**.
The shared key is used to encrypt the connection between the Management Server and the Firebox SOHO. This shared key must be the same on the SOHO and the Management Server. You must get the shared key from your Management Server administrator.

12 Click **Submit.**
When you save the configuration to the Firebox SOHO, the SOHO is enabled as a managed client. The managed SOHO client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed SOHO client.

Adding Devices to the Management Server

You can use the Management Server to configure and manage VPN tunnels between Firebox® devices, including Firebox III and Firebox X Core devices that use WFS appliance software, Firebox X devices that use Fireware® appliance software, Firebox X Edge devices, and Firebox SOHO devices.

A device with a dynamic IP address must also be configured as a Managed Client from Policy Manager for the device. See the previous section for these instructions.

If your device has multiple external interfaces, do not change the interface configuration after you add the device to the Management Server.

Note

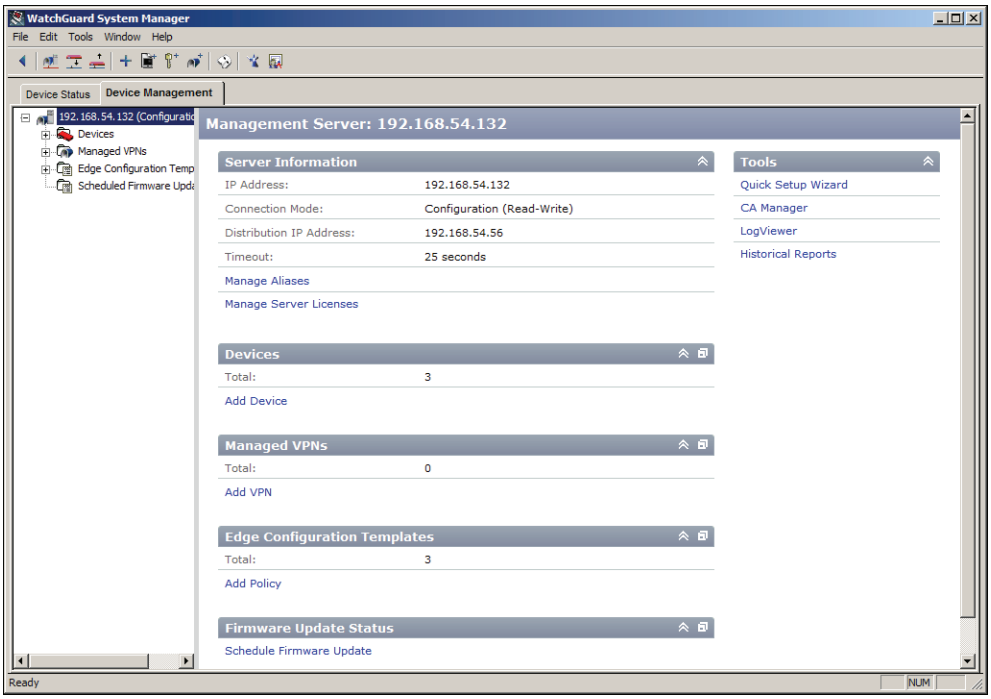
With the Management Server, you can also deploy, manage, and monitor Firebox X Edge devices. See the “Managing the Firebox X Edge and Firebox SOHO” chapter for more information.

1 In WatchGuard® System Manager, connect to the Management Server.
Select File > Connect to Server, or select the Device Status tab.
Or
Right-click anywhere in the window and select Connect to > Server.

2 Type or select the IP address of the Management Server, type the passphrase, and click **Login**.

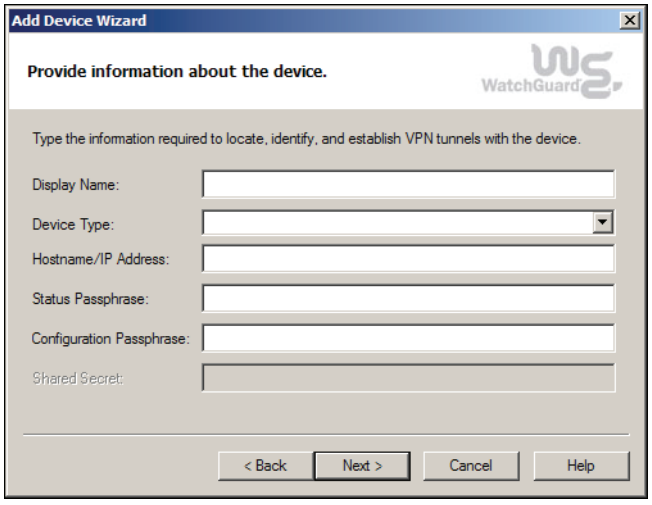
3 Click the **Device Management** tab.

4 Select the Management Server from the list at the left of the window.
The Management Server page appears.



5 Expand the **Devices** folder.
All devices managed by this Management Server are shown here.

6 Select **Edit > Insert Device**, or right-click in the left frame of this window and select **Insert Device**.
The Add Device wizard starts.



7 Click **Next** to see the first configuration screen.

8 In the **Display Name** text box, type a name for the device.
This name cannot include any spaces or the period (dot) character.

9 From the **Device Type** drop-down list, select the model of the Firebox you want to add to the Management Server configuration.

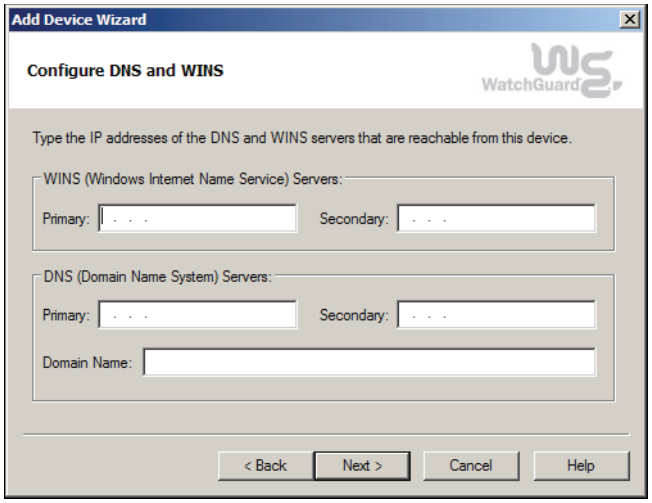
10 In the **Hostname/IP address** text box, type the static IP address or host name of the Firebox. For devices that use a dynamic IP address, type the Dynamic DNS service client name.
If the device has a dynamic IP address but does not use the Dynamic DNS service, type a unique name for the device. The name you type here must match the name you enter in Policy Manager for that device (if the device is a Firebox III, Firebox X Core or X Peak). If the device is a Firebox X Edge or SOHO, this name must match the name you give the device when you enable the device as a managed client with the web configuration manager.

11 Type the status passphrase. This is the status (read-only) passphrase for the Firebox you are adding to the Management Server.

12 Type the configuration passphrase. This is the configuration (read-write) passphrase for the Firebox you are adding to the Management Server.

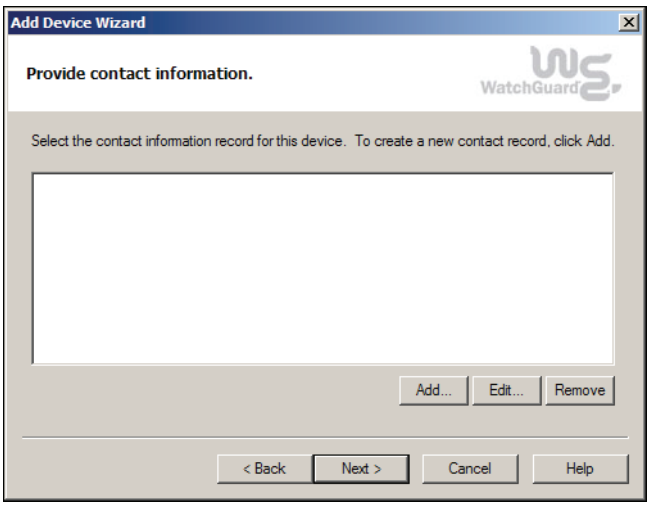
13 If the Firebox uses a dynamic IP address, type the shared secret. The shared secret you type here must match the shared secret you type in the device's configuration when you enable it as a managed client.

14 Click **Next**.
The Configure WINS and DNS screen appears.



15 Type primary and secondary addresses for the WINS and DNS servers this device uses, if any.

16 Type the domain name for this device, if any. Click **Next**.
The Provide Contact Information screen appears.



17 You can select an existing contact record for this device, or click **Add** to add a new contact record for this device. You can also delete an existing contact record: select it and click **Delete**.

18 Click **Next**. The Configure the Device screen appears. Click **Next** on this screen to configure the device with the new management settings and add it to the Management Server. If the device is already managed by another server, or configured for management by this server, a warning dialog box appears. Click **Yes** to continue.

19 Click **Close** to close the Add Device wizard.
After you add a Firebox with a dynamic IP address, you must restart that Firebox so that it can connect to the Management Server to get its configuration.

Note

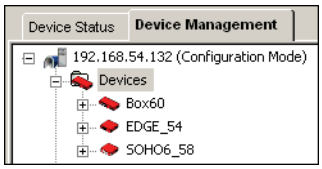
If traffic is very heavy, the Add Device wizard cannot connect because of SSL time-out. Try again later when the system has less load.

Using the Device Management Page

When a Firebox® is added to a Management Server, you can use the information and fields on the **Device Management** tab to configure settings on the device. For more information about how to add a device to the Management Server, see "Adding Devices to the Management Server" on page 213.

Viewing the Firebox management page

1 Expand **Devices** in the WatchGuard® System Manager **Device Management** tab.
A list of managed devices appears.



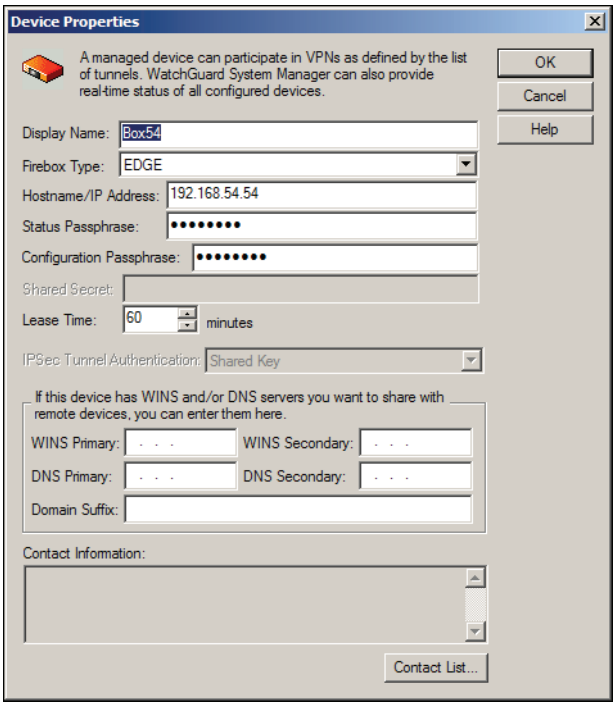
2 Select a Firebox. The management page for the device appears.

Note

The management page for a Firebox X Edge device allows you to get access to different tools and configure more options. For Firebox X Edge management information, see the "Managing the Firebox X Edge and Firebox SOHO" chapter.

Configuring Firebox management properties

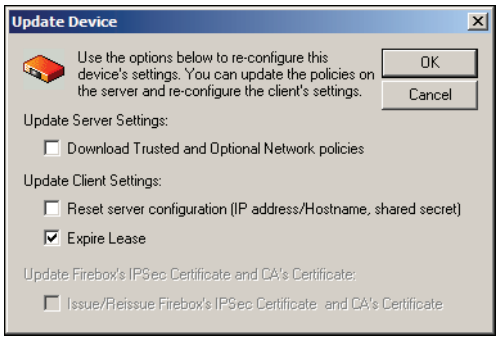
1 On the Firebox management page, click **Configure**.
The Device Properties dialog box appears.


Device Properties
A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.
OK
Cancel
Help
Display Name: Box54
Firebox Type: EDGE
Hostname/IP Address: 192.168.54.54
Status Passphrase:
Configuration Passphrase:
Shared Secret:
Lease Time: 60 minutes
IPSec Tunnel Authentication: Shared Key
If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.
WINS Primary:
WINS Secondary:
DNS Primary:
DNS Secondary:
Domain Suffix:
Contact Information:
Contact List...

2 Configure the management properties for the device.

Updating the device

1 On the Firebox management page, click **Update Device**.
The Update Device dialog box appears.


Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

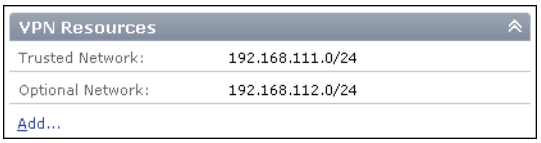
2 Use this dialog box to get the policies from the device, to set the Management Server configuration for the device, and to expire the management lease. You also can use this dialog box to update the Firebox certificate and the CA certificate, if they have changed.

3 Click **OK**.

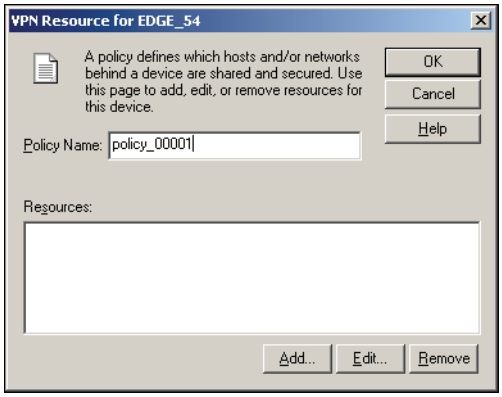
Adding a VPN resource

A VPN resource is a secure IP address or network address that VPN users can connect to.

1 On the **Device Management** tab, find the **VPN Resources** section.



2 Click **Add**.


VPN Resource for EDGE_54
A policy defines which hosts and/or networks behind a device are shared and secured. Use this page to add, edit, or remove resources for this device.
OK
Cancel
Help
Policy Name: policy_00001
Resources:
Add...
Edit...
Remove

3 Use the appropriate buttons to add, edit, or remove VPN resources.

4 Click **OK**.
The new VPN resource appears on the list.

Starting Firebox tools

The **Device Management** tab allows you to start four tools for Firebox configuration and monitoring:

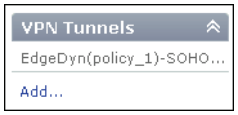
- Policy Manager
- Firebox System Manager
- HostWatch
- Ping

To start these tools, click the link for the tool from the Tools section on the Firebox management page.

Adding a Firebox VPN tunnel

The tunnels section of the Firebox management page shows all tunnels for which the device is an end-point. You can also add a VPN tunnel in this section.

1 On the Firebox management page, find the VPN Tunnels section.



2 Click **Add** to add a new VPN tunnel.
The Add VPN Wizard starts. Follow the prompts in the wizard to configure the VPN.

Monitoring VPNs

Manually configured VPNs are shown in the **Device Status** tab for each Firebox®. Managed VPNs that are created automatically on a Management Server appear on the **Device Management** tab.

VPN policies that you create manually with Policy Manager are not shown on the **Device Management** tab.

CHAPTER 17

Managing Certificates and the Certificate Authority

When you create a VPN tunnel, you can select from two types of tunnel authentication: shared secrets or certificates. Shared secrets are an authentication method used to create trust between computers in a VPN. A shared secret is used with a passphrase. Certificates usually give more security than shared secrets during the authentication procedure.

A certificate is an electronic document that contains a public key. A Certificate Authority (CA) is a trusted third party that gives certificates to clients. In WatchGuard® System Manager, the workstation that is configured as the Management Server also operates as a CA. The CA can give certificates to managed Firebox® clients when they contact the Management Server to receive configuration updates.

Certificate Authorities are a component of a system of key creation, key management and certification with the name Public Key Infrastructure (PKI). The PKI supplies certificate and directory services that can create, supply, keep, and when necessary revoke the certificates.

Public Key Cryptography and Digital Certificates

Public key cryptography is a central component of a PKI. This cryptographic system includes two mathematically related keys, known as an asymmetric key pair. The user keeps one key, the private key, secret. The user can supply the other key, known as the public key, to other users.

The keys in the key pair go together. Only the owner of the private key can decrypt data encrypted with the public key. Any person with the public key can decrypt data encrypted with the private key.

Certificates are used to make sure public keys are valid. Certificates contain a digital signature created with the public key of a CA certificate. To make sure a certificate is legitimate, you can get the CA public key. You can compute the digital signature of the certificate and compare it to the digital signature in the certificate itself. If the signatures match, the key is legitimate.

Certificates have a lifetime that is set when they are created. But certificates are occasionally revoked before the end date and time that was set for their lifetime. The CA keeps an online, current list of revoked certificates. This list is the certificate revocation list (CRL).

PKI in a WatchGuard VPN

To authenticate VPN tunnels with certificates, you must first configure a Management Server. When you configure the Management Server, the CA is automatically activated. Each managed Firebox® client connects to the Management Server and receives a certificate from the CA. When a VPN tunnel is created between two managed clients, the clients use the certificates to authenticate the tunnel. This occurs only if each of the two managed Firebox clients is configured to use certificate authentication.

MUVPN and certificates

Because mobile user VPN (MUVPN) clients are not clients of the Management Server, they authenticate to the Firebox. Use the MUVPN Wizard from Policy Manager to contact the CA and create a certificate for the MUVPN client. Policy Manager creates a package that includes this certificate and two other files.

The Firebox administrator gives each MUVPN user the package of files. Together, these files are the MUVPN end-user profile. Users who authenticate with shared keys receive one .wgx file. Users who authenticate with certificates receive a .wgx file, a .p12 file (which is the client certificate), and a cacert.pem file (which contains the root certificate).

The MUVPN user who authenticates with certificates then opens the .wgx file. The root and client certificates contained in the cacert.pem and the .p12 files are automatically loaded.

For more information on MUVPN, see the *MUVPN Administrator Guide*.

Managing the Certificate Authority

You can control different parameters of the Certificate Authority with the web-based CA Manager.

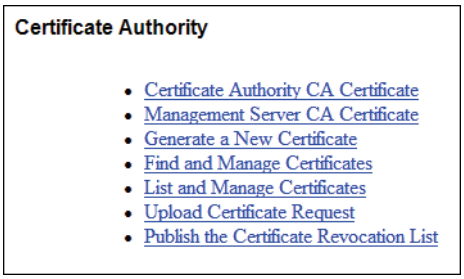
1 From WatchGuard® System Manager, connect to the Management Server.
You must type the configuration passphrase to connect.

2 Click the **Device Management** tab for the Management Server.

3 Below the **Tools** menu, select **CA Manager**.

or
Click the CA Manager icon on the WatchGuard System Manager toolbar. The icon is shown at left.

The menu of the Certificate Authority Settings pages appears.



4 From the menu, select the correct page:

Certificate Authority CA Certificate
Print a copy of the CA (root) certificate to the screen. You can manually save it to the client.

Management Server CA Certificate

Print a copy of the Management Server CA certificate to the screen. You can manually save it to the client. You can use this for client access to the authentication web page.

Generate a New Certificate

Type a subject common name, organizational unit, password, and certificate lifetime to make a new certificate.

- For MUVPN users, the common name must agree with the user name of the remote user.
- For Firebox® users, the common name must agree with the Firebox identifying information (normally, its IP address).
- For a generic certificate, the common name is the name of the user.

Note

Type the organizational unit only if you make certificates for MUVPN users. Do not use this for other types of VPN tunnels. The unit name must appear in this format:
GW:<*vpn gateway name*>
where <*vpn gateway name*> is the value of config.watchguard.id in the configuration file of the gateway Firebox.

Find and Manage Certificates

Give the serial number, common name, or organizational unit of a certificate to find in the database. Also, as an alternative to a special certificate, you can make sure that only active, revoked, or expired certificates are found. The results of the search appear on the List Certificates page.

List and Manage Certificates

See a list of certificates that are in the database. Select the certificates to publish, revoke, put back, or remove. For information about how to manage certificates, see the section that follows.

Upload Certificate Request

Use this page to sign a certificate request from a different device. Type in the common name and organizational unit of the subject and click **Browse** to find the CSR (Certificate Signing Request) file.

Publish a Certificate Revocation List (CRL)

Make the CA publish the CRL to all clients with current certificates. A Managed Firebox client cannot create a VPN tunnel if it uses a certificate that is on the CRL to authenticate.

Managing certificates with the CA Manager

You use the List and Manage Certificates page to publish, revoke, put back, or remove certificates:

1 From the List and Manage Certificates page, select the serial number of the certificate to change.

2 From the **Choose Action** drop-down list, select one of the alternatives, and then select **GO**:

Revoke Checked

Revokes a certificate. Managed Firebox clients will not see that the CRL was revoked until the CRL is published.

Reinstate Checked

Puts back a certificate that was revoked before.

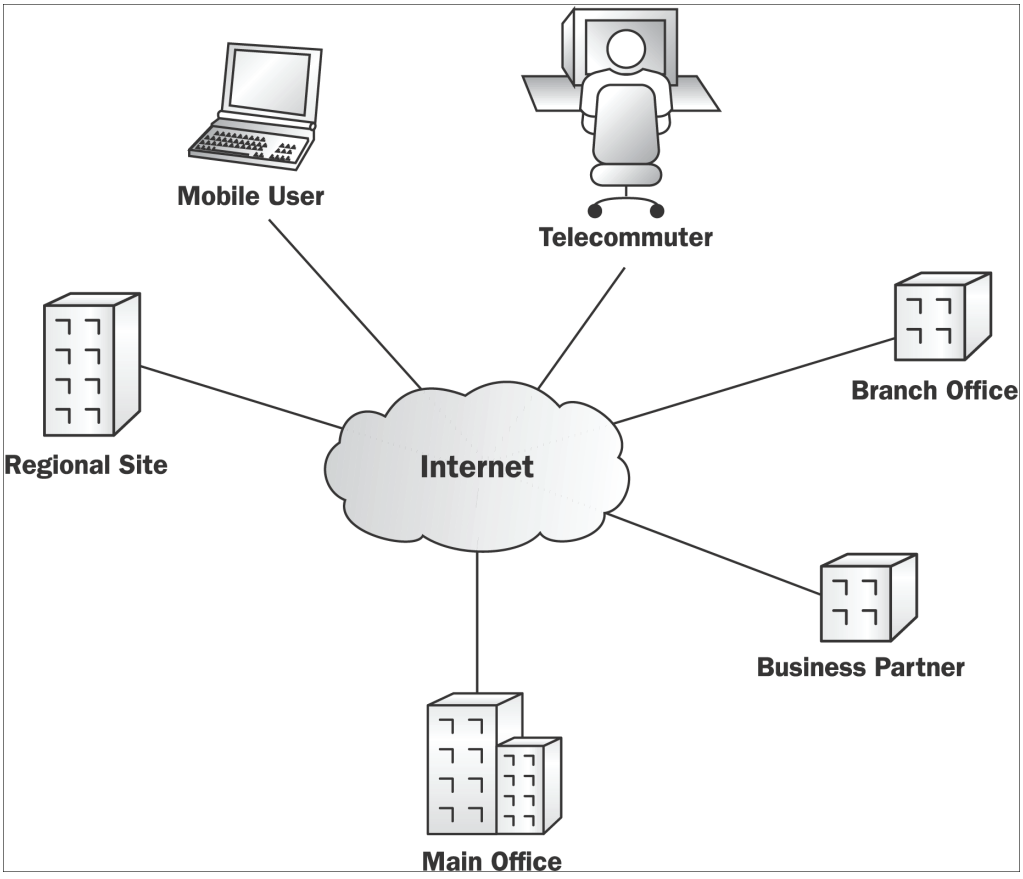
Destroy Checked

Removes a certificate.

CHAPTER 18

Introduction to VPNs

The Internet is a public network. On this system of computers and networks, one computer can get information from other computers. It is possible for a person to read unsecured data packets that you send on the Internet. To send secure data on the Internet between offices, networks, and users, you must use stronger security.



Virtual private networks (VPNs) use encryption technology to decrease security risks, and to secure private information on the public Internet. A virtual private network lets data flow safely across the Internet between two networks. VPN tunnels can secure connections between a host and a network.

The networks and hosts at the endpoints of a VPN can be corporate headquarters, branch offices, and remote users.

VPN tunnels use authentication, which examines the sender and the recipient. If the authentication information is correct, the data is decrypted. Only the sender and the recipient of the message can read it clearly.

For more information on VPN technology, see the online information at:

http://www.watchguard.com/support

The WatchGuard® Support web site contains links to documentation, basic FAQs, advanced FAQs, and the WatchGuard User Forum. You must log in to the Technical Support web site to use some features.

Tunneling Protocols

Tunnels allow users to send data in secure packets across a network that is not secure, usually the Internet. A tunnel is a group of security protocols, encryption algorithms, and rules. The tunnel uses this information to send secure traffic from one endpoint to the other. A tunnel allows users to connect to resources and computers from other networks.

Tunneling protocols supply the infrastructure and set how the data transmission on the tunnel occurs. The two tunneling protocols that WatchGuard® System Manager supports are Internet Protocol Security (IPSec) and Point-to-Point-Tunneling Protocol (PPTP). WatchGuard also supports SSL VPN with its WatchGuard SSL VPN Firebox product line.

IPSec

You use the IPSec protocol to examine IP packets and make sure they are authenticated. IPSec includes security features including very strong authentication to protect the privacy of the information that you transmit on the Internet. IPSec is a standard that works with many systems from different manufacturers.

IPSec includes two protocols that protect data integrity and confidentiality. The AH (Authentication Header) protocol is the solution for data integrity. The ESP (Encapsulated Security Payload) protocol gives data integrity and confidentiality.

PPTP

Point to Point Tunneling Protocol (PPTP) is a standard for VPN security that can be used with many systems from different manufacturers. PPTP allows tunnels to corporate networks and to other PPTP-enabled systems. PPTP is not as secure as IPSec and cannot secure two networks. PPTP can only secure one IP address with one other IP address or with a network. PPTP supplies an inexpensive tunnel alternative for a corporate network that is easier to use than IPSec.

Encryption

On a network that is not secure, hackers can find transmitted packets very easily. VPN tunnels use encryption to keep this data secure.

The length of the encryption key, together with the algorithm used, set the encryption strength for the VPN. A longer key gives better encryption and more security. The level of encryption is set to give the performance and security that is necessary for the organization. Stronger encryption usually gives a higher level of security, but can have a negative effect on performance.

Basic encryption allows sufficient security with good throughput for tunnels that do not transmit sensitive data. For administrative connections and for connections where privacy is very important, we recommend strong encryption.

The host or the IPSec device that sends a packet through the tunnel encrypts the packet. The recipient at the other end of the tunnel decrypts the packet. The two endpoints must agree on all the tunnel parameters. This includes the encryption and authentication algorithms, the hosts or networks allowed to send data across the tunnel, the time period for calculating a new key, and other parameters.

Selecting an encryption and data integrity method

Think of security and performance when you select the encryption and data integrity algorithms to use. We recommend Advanced Encryption Standard (AES), the strongest of the encryption types, for sensitive data. Fireware® uses AES 256 as the default encryption algorithm for IPSec.

Data integrity makes sure that the data a VPN endpoint receives is not changed as it is sent. We give support to two types of data authentication. The first type is 128-bit Message Digest 5 (MD5-HMAC). The second type is 160-bit Secure Hash Algorithm (SHA1-HMAC).

Authentication

An important part of security for a VPN is to make sure that the sender and recipient are authenticated. There are two method: passphrase authentication (also called a shared secret) and digital certificates. A shared secret is a passphrase that is the same for the two ends of the tunnel.

Digital certificates use public key cryptography to identify and authenticate the end gateways. You can use certificates for authentication for any VPN tunnel you create with your WatchGuard Management Server. For more information on the certificates, see the "Managing Certificates and the Certificate Authority" chapter.

Extended authentication

Authentication for a remote user can occur through a database that is kept on the Firebox®, or through an external authentication server. An example of an external authentication server is the Remote Authentication Dial-In User Service (RADIUS). An authentication server is a safe third party that authenticates other systems on a network. With Mobile User VPN (MUVPN), which uses the IPSec tunneling protocol, the remote user must type a user name and password each time a VPN is started.

Selecting an authentication method

A primary part of a VPN is its method of user authentication. When you use shared secrets safely, you must make sure that you:

- Make users select strong passwords.
- Change passwords frequently.

When you use Remote User VPN (RUVPN), which uses the PPTP tunneling protocol, or MUVPN, it is very important to use strong passwords. When you put the security of VPN endpoints at risk, you can put the

security of the network at risk. If, for example, a person steals a laptop computer and finds the password, that person has direct access to the network.

Digital certificates are electronic records that identify the user. For more information about certificates, see the "Managing Certificates and the Certificate Authority" chapter. The Certificate Authority (CA), a safe third party, manages the certificates. In the WatchGuard® System Manager, you can configure a Firebox to operate as a CA. This type of authentication can be safer than shared secrets.

IP Addressing

Correct use of the IP address is important when you make a VPN tunnel. It is best if the private IP addresses of the computers at one side of the VPN tunnel are not the same as the private IP addresses used at the other side of the VPN tunnel. If you have branch offices, use subnets at each location that are different from the primary office network. If it is possible, use subnets that are almost the same as the Firebox® subnet when you set up a branch office.

For example, if the primary Firebox network uses 192.168.100.0/24, then for the branch offices use 192.168.101.0/24, 192.168.102.0/24, and so on. This prevents new problems if you expand your network, and it helps you remember the IP addresses at your branch offices.

For MUVPN and RUVPN tunnels, the Firebox gives each remote user a virtual IP address. The easiest method is to give virtual IP addresses that come from the primary network but are not used for any other computer. You cannot use the same virtual IP address for RUVPN and for MUVPN remote users. You also cannot use a virtual IP address that can be on a computer at a different location on the primary network.

If your primary network does not have sufficient IP addresses to do this, the safest procedure is to install a "placeholder" secondary network. Select a range of addresses for it and use an IP address from that range for the virtual IP address. If you are already using a private IP address range on your primary network, you can also expand the network range. For example, you can change from the class C network 192.168.100.0/24 to a class B network of 192.168.0.0/16.

This lets you select from a range of addresses. There is no interference from these addresses with real host addresses in use behind the Firebox. If you use this procedure for RUVPN virtual IP addresses, you must configure the client computer to use the default gateway on the remote network, or you must manually add routes after the VPN tunnel is connected. This is not necessary for the MUVPN client computer.

Internet Key Exchange (IKE)

As the number of VPN tunnels in your network increases, it can get more difficult to manage the large number of session keys that are used by the tunnels. Keys must be replaced frequently for stronger security.

Internet Key Exchange (IKE) is the key management protocol IPSec uses. IKE automates the procedure to negotiate and replace keys. The Internet Security Association and Key Management Protocol (ISAKMP) is a cryptographic protocol that is the basis of the IKE key interchange protocol. This protocol uses a two-phase procedure to create an IPSec tunnel. During Phase 1, two gateways create a safe, authenticated channel for VPN traffic. Phase 2 includes an interchange of keys to find out how to encrypt the data between the two.

Diffie-Hellman is an algorithm that IKE uses to make keys that are necessary for data encryption. Diffie-Hellman groups are collections of parameters. These groups let two peer systems interchange and

agree on a session key. Group 1 is a 768-bit group, and group 2 is a 1024-bit group. Group 2 is more secure than group 1, but uses more processor time to make the keys.

Network Address Translation and VPNs

With Network address translation (NAT), the source and destination addresses of IP packets are changed as they go through the router or a firewall. If you use NAT between two VPN gateways, you must use ESP (not AH) as the authentication protocol when you create VPN tunnels between the devices.

If you send IPSec or PPTP traffic through a Firebox® (IPSec or PPTP pass-through), the Firebox can use 1-to-1 NAT to send the traffic.

Access Control

VPN tunnels lets users get access to resources on your computer network. Think which type of resources are needed by a given type of user. For example, you can let a group of contract employees get access to only one network and your sales personnel can get access to all the networks.

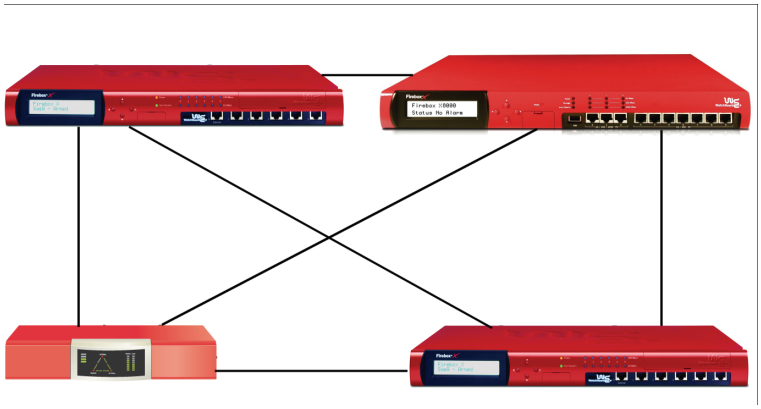
Different VPN types also can set your level of trust. Branch office VPNs (BOVPNs) have a firewall device at the two ends of the tunnel. They are more safe than MUVPN and RUVPN, which have protection at only one end.

Network Topology

You can configure the VPN for support of meshed and hub-and-spoke configurations. The topology that you select sets the types and number of connections that occur. It also sets the flow of data and the flow of traffic.

Meshed networks

In a fully meshed topology, all servers are connected together to make a web. Each device is only one step from each other VPN unit. Traffic can go between each unit of the VPN, if necessary.



Fully Meshed Network

This topology is the most error resistant. If a VPN unit goes down, only the connection to the trusted network of that unit is down. But, this topology is more work to set up. Each VPN unit must have a VPN tunnel configured to each other unit. There can be possible routing problems if it is not done carefully.

The largest problem that you get with fully meshed networks is one of control. Because each unit in the network must connect with each other unit, the number of necessary tunnels becomes large quickly. The number of tunnels that are necessary for this configuration is the same as the square of the number of devices:

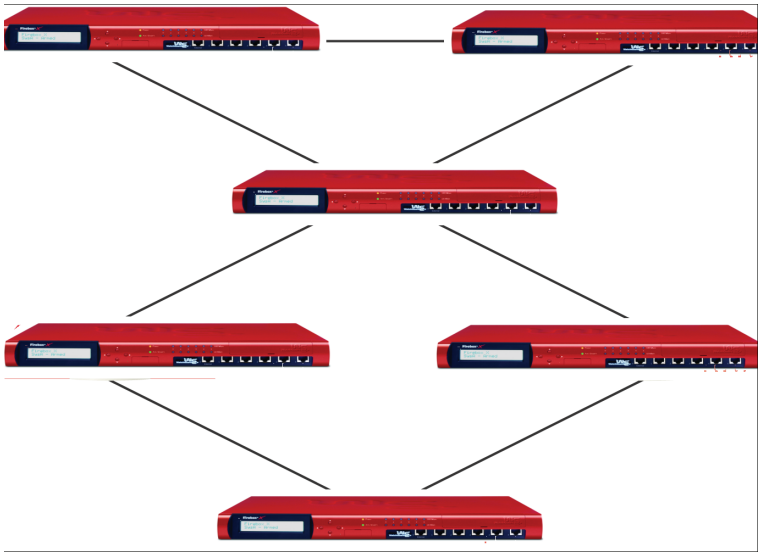
[(number of devices) x (number of devices)] -1 ÷ 2 = number of tunnels]

When all the VPN units are WatchGuard® devices, WatchGuard System Manager can make it easy to set up. The Management Server contains all the information for all the tunnels. With WatchGuard System Manager, you make a VPN tunnel between two devices in three steps using a drag-and-drop method.

You can monitor the security of the full system from more than one location, each with a Firebox®. Larger companies use this configuration with important branch offices, each using a higher capacity Firebox. Smaller offices and remote users connect with MUVPN, RUVPN, Firebox X Edge, or SOHO 6 devices.

Networks that are not fully meshed have only the necessary inter-spoke VPN tunnels. Refer to the figure below. Thus the flow through the network is better than fully meshed networks. The limits in all meshed networks are:

- The number of VPN tunnels that the firewall CPU can operate.
- The number of VPN tunnels allowed by the VPN license on the unit.



Partially Meshed Network

Hub-and-spoke networks

In a hub-and-spoke configuration, all VPN tunnels stop at one firewall. Smaller companies frequently use this configuration with a primary Firebox. Many distributed remote users connect with MUVPN, RUVPN, Firebox X Edge, or SOHO 6 devices to this configuration. Each remote device or remote user makes a VPN tunnel only to the primary Firebox.

In a simple hub-and-spoke configuration, each remote location can send and receive data only through a VPN tunnel to the network behind the primary Firebox. A VPN tunnel to the primary Firebox can also

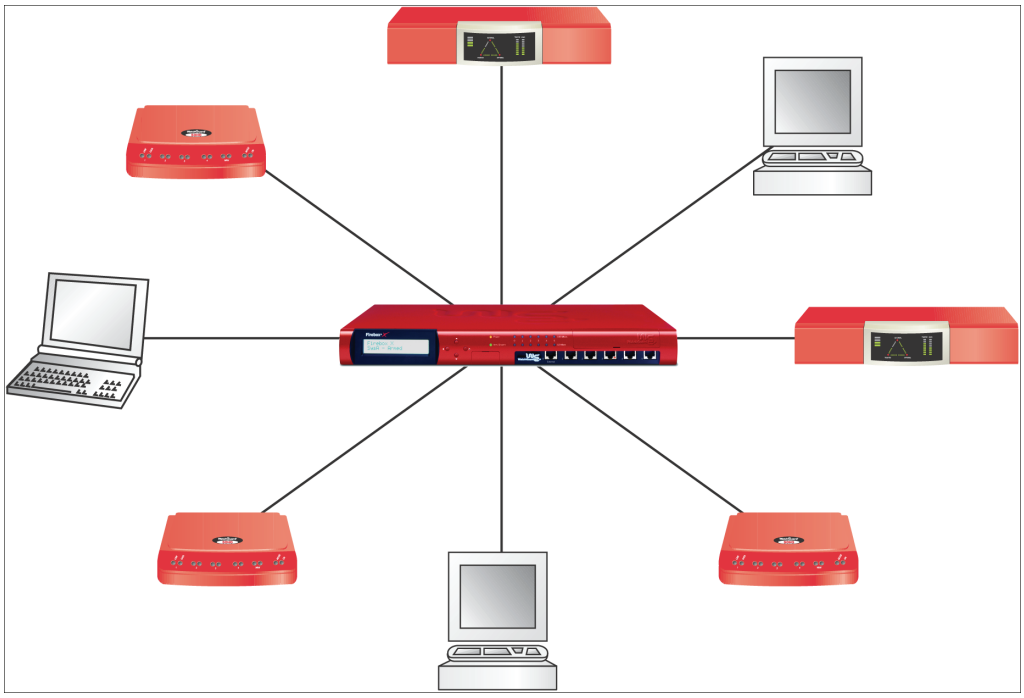
be configured to send and receive data to a different remote VPN location (tunnel switching). The intensity of traffic in hub-and-spoke can be high if the primary Firebox sends packets from one remote location to a different remote location. The traffic intensity also can be low in a simple hub-and-spoke, where the remote locations can only send data through a VPN tunnel to the primary hub location.

The primary Firebox is the one point where all VPN tunnels can fail, so it can be a problem. If it goes down, you cannot connect any VPN tunnels to the remote locations.

The flow through a simple hub-and-spoke system is far more clear than through a meshed system. You can control the number of tunnels better. Refer to the sum that follows:

[(number of devices) – 1 = number of tunnels]

If it is necessary to have more spoke capacity, you expand the hub location. But, because all traffic goes through the hub, it is necessary to have more bandwidth for this installation.



Hub and Spoke Network

Tunneling Methods

Split tunneling is when a remote user or endpoint has access to the Internet on the same computer as the VPN connection. But, this user does not put the Internet traffic through the tunnel. The remote user browses directly through the ISP. This makes the system vulnerable, because Internet traffic is not filtered or encrypted.

This dangerous configuration is less vulnerable when all of the Internet traffic of the remote user goes through a VPN tunnel to the Firebox®. From the Firebox, the traffic is then sent back out to the Internet (tunnel switching). With this configuration the Firebox examines all traffic and gives better security.

When you use tunnel switching, a Dynamic NAT policy must include the outgoing traffic from the remote network. This allows the remote users to browse the Internet when they send all traffic to the Firebox.

Split tunneling decreases security, but does increase performance. If you use split tunneling, remote users must have personal firewalls for computers behind the VPN endpoint.

WatchGuard VPN Solutions

WatchGuard® System Manager includes this software to create tunnels:

- Remote User VPN (RUVPN) with PPTP
- Mobile User VPN (MUVPN) with IPSec
- Branch Office VPN (BOVPN) with IPSec, which uses Policy Manager to manually configure the tunnel settings
- Branch Office VPN (BOVPN) with IPSec, which uses WatchGuard System Manager to automatically configure the tunnel settings.

WatchGuard includes different types of encryption for the different types of VPN tunnels you can create. BOVPN allows Data Encryption Service (DES) with a 56-bit encryption key for basic encryption, 112-bit key for moderate encryption, and a 168-bit encryption key (3DES) for strong encryption. It also allows the Advanced Encryption Standard (AES), a block data encryption method, using 128-bit, 192-bit, or 256-bit encryption.

WatchGuard also has an separate SSL VPN Firebox product line. You can see more information on the WatchGuard public web site at http://www.watchguard.com/products/fb-ssl.asp.

Remote User VPN with PPTP

Remote User VPN allows remote users or mobile users to connect to the Firebox® network with PPTP. RUVPN with PPTP allows RC4 40-bit or 128-bit keys.

The basic WatchGuard System Manager package includes RUVPN with PPTP. It allows 50 users, and all levels of encryption. For information on how to create RUVPN with PPTP tunnels, see the "Configuring RUVPN with PPTP" chapter.

Mobile User VPN

Note

For information on how to configure and use MUVPN, see the MUVPN Administrator Guide.

Mobile User VPN is an optional software component available for all Firebox models. Remote users are mobile employees who must have corporate network access. MUVPN creates an IPSec tunnel between a remote host that is not secure and your corporate network. Remote users connect to the Internet with a standard Internet dial-up or broadband connection, and then they use the MUVPN software to make a secure connection to the network or networks protected by the Firebox. With MUVPN, only one Firebox is necessary to create the tunnel.

MUVPN uses IPSec with DES or 3DES to encrypt incoming traffic, and MD5 or SHA-1 to authenticate data packets. You configure a security policy and supply it along with the MUVPN software to each remote user. The security policy is an encrypted file with the extension wgx. When the software is installed on the computers of the remote users, they can safely connect to the corporate network. MUVPN users can change their security policies, or you can give them read-only security policies.

Branch Office Virtual Private Network (BOVPN)

Many companies have offices in more than one location. Offices frequently use data from other locations, or have access to shared databases.

Because branch offices have sensitive company data, information interchanges must be secure. When you use WatchGuard Branch Office VPN, you can connect two or more locations across the Internet without decreasing security. WatchGuard BOVPN supplies an encrypted tunnel between two networks or between a Firebox and an IPSec-compliant device. You can use WatchGuard System Manager or Policy Manager to configure BOVPN.

WatchGuard allows certificate-based authentication for BOVPN tunnels. When you use certificate-based authentication for BOVPN, the two VPN endpoints must be WatchGuard Fireboxes. You cannot use certificate-based authentication for BOVPN with SOHO 6 or Firebox X Edge devices. To use this functionality, you must configure a Management Server and a certificate authority. For more information, see "Configuring Managed VPN Tunnels," on page 169. For instructions on how to use Policy Manager to manually configure a BOVPN tunnel, see "Configuring BOVPN with Manual IPSec," on page 161.

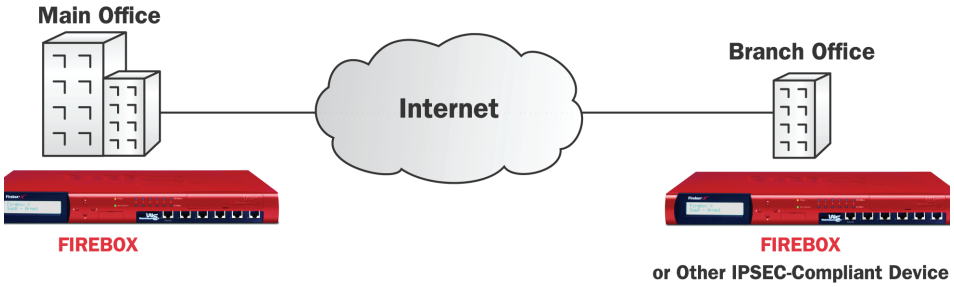
BOVPN with Policy Manager

When you make a tunnel with Policy Manager, the Firebox uses IPSec to make encrypted tunnels with a different IPSec-compliant security device. One of the two endpoints must have a public static IP address. Use BOVPN with Policy Manager if:

- You make tunnels between a Firebox and a non-WatchGuard, IPSec-compliant unit.
- You give different routing policies to different tunnels.
- Not all types of traffic go through the tunnel.

BOVPN with IPSec is available with the moderate encryption level of DES (56-bit), or the stronger encryption 3DES (168-bit). BOVPN is also available with AES at the 128-bit, 192-bit, and 256-bit encryption levels. AES with 256-bit encryption is the most secure.

You can create different VPN tunnels for different types of traffic on your network. For example, you can use a VPN tunnel with DES encryption for traffic from your sales team. At the same time use a VPN tunnel with stronger, 3DES encryption for all data from your finance department.



BOVPN with Manual IPSec

BOVPN with WatchGuard System Manager

With WatchGuard System Manager, you can make fully authenticated and encrypted IPSec tunnels with a drag-and-drop or menu interface. WatchGuard System Manager uses the Management Server to safely transmit IPSec VPN configuration information between two Firebox devices. When you use the Management Server, you set each configuration parameter of the VPN. The Management Server keeps this information.

Use BOVPN with WatchGuard System Manager if:

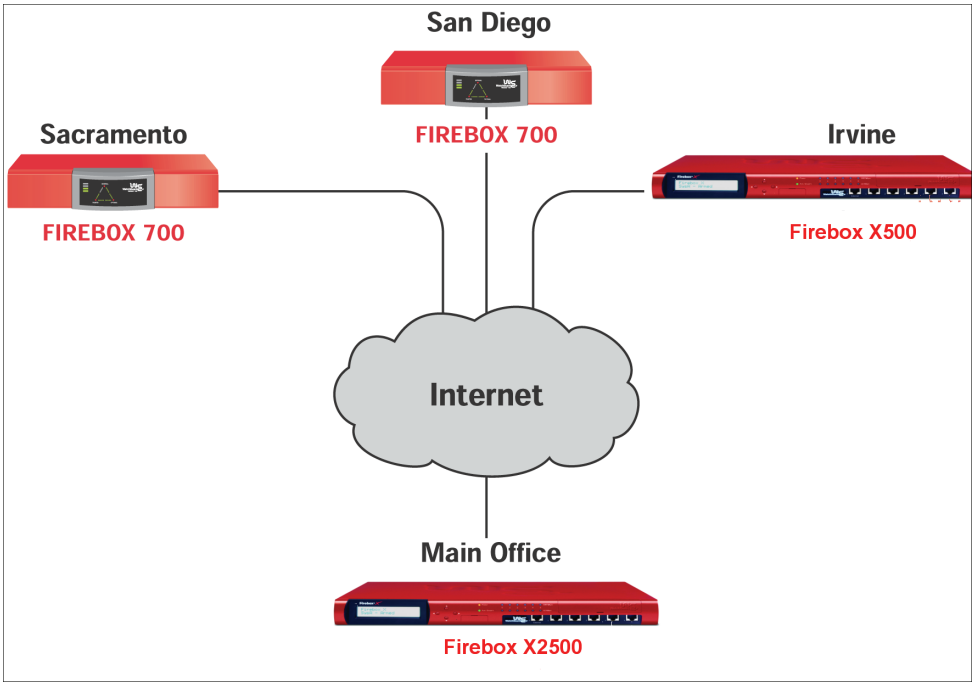
- You make tunnels between two or more Firebox devices.
- You give different routing policies to different tunnels.
- Client units have dynamic or static public IP addresses.
- You have a large number of tunnels to make.

With WatchGuard System Manager you can configure, manage, and monitor all WatchGuard devices across a company. You can configure VPN tunnels between two remote devices easily, using the default settings that WSM gives you. You do not have to know about the Internet security of branch offices and remote users. Remote devices connect to the Management Server, and WSM does all the work. If you use certificates for tunnel authentication, you can configure the Management Server as a certificate authority to create certificates automatically.

VPN Scenarios

This section gives three different types of companies and the VPN solutions that best fit each one.

Large company with branch offices: WatchGuard System Manager



Large Company with VPNs to Branch Offices

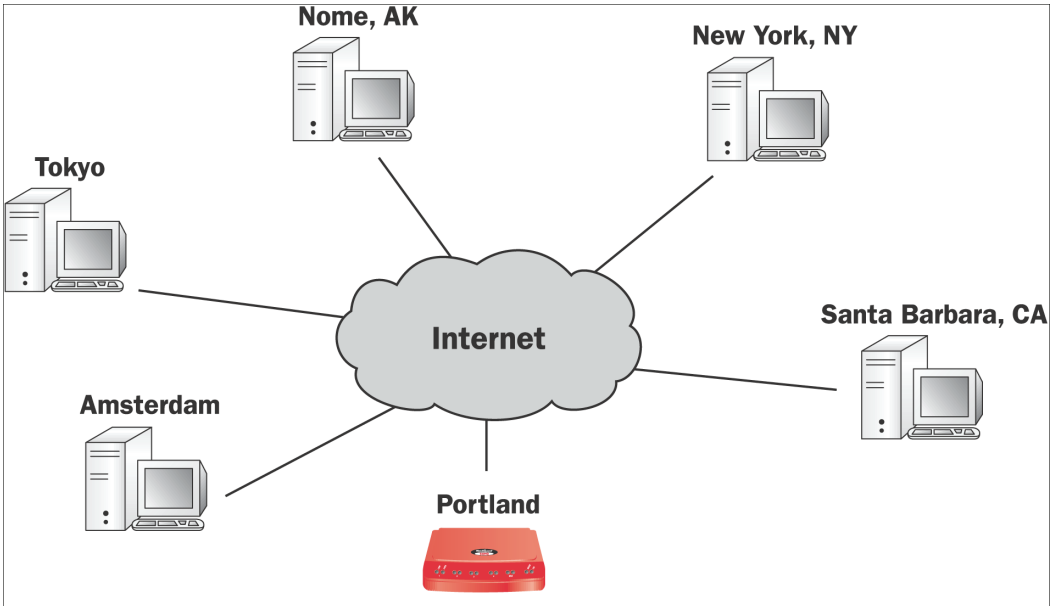
Gallatin Corporation has a head office with approximately 300 users in Los Angeles. It has branch offices of approximately 100 users each in Sacramento, San Diego, and Irvine. All locations have high-speed access to the Internet and employees at all locations must have secure connections to all other locations.

This company usesa WatchGuard Firebox® at each location and WatchGuard® System Manager to connect the locations to each other. Each office connects to all other offices. All users at each office have access to the shared records at all the other locations. The Management Server is behind the Firebox at

the primary office, and the Fireboxes at the branch offices are Managed Firebox Clients. When a service stop occurs with Gallatin's Internet service provider, it makes the Firebox at headquarters unavailable. But the tunnels in the other locations stay active.

Small company with telecommuters: MUVPN

River Rock Press is a small publishing company in a specialty market. It has an office with six employees in Portland, Oregon, and five editors who are in other locations. The head office uses a Firebox X Edge as a firewall and as a VPN gateway. The five editors each use a MUVPN client to make a secure connection to the Information Center in Portland. The editors can always safely interchange information if their computers are connected to the Internet.



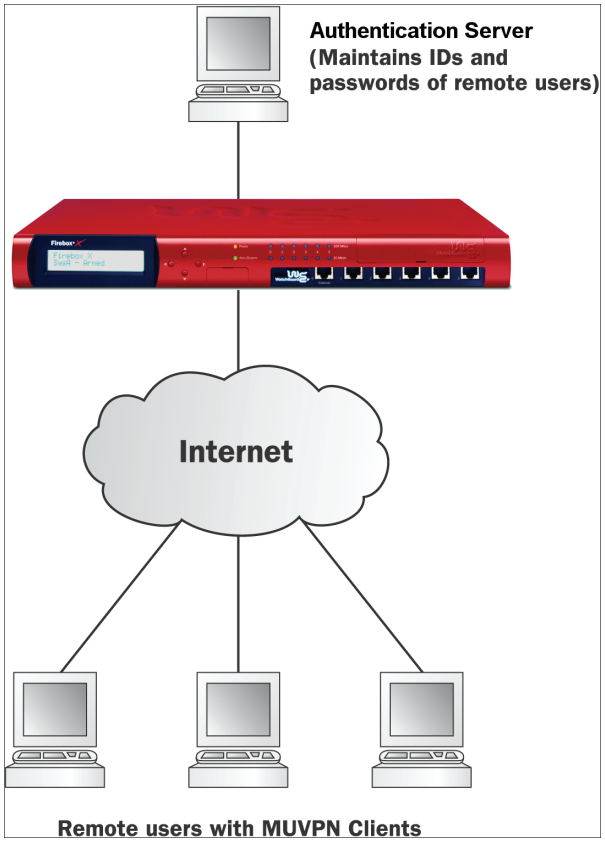
Small Company with Telecommuters Using Mobile User VPN

Company with remote employees: MUVPN with extended authentication

BizMentors, Inc. has 35 trainers to give classes on business topics at the locations of client companies. The 75 salespeople of BizMentors must have current information on the schedules of the trainers to prevent conflicts.

A database in the data center of BizMentors keeps this information current. The data center uses a Firebox and each salesperson uses an MUVPN client to get access to the inventory and price database. To authenticate all remote users, BizMentors uses a RADIUS authentication server.

Usually, you must enter the ID and password information on the Firebox and on the authentication server. But when you use extended authentication, all IDs and passwords are sent to the authentication server. You do not have to put them in the Firebox. All salespersons can log in to the corporate network with the ID and password they usually use when inside the network. The Firebox sends the ID and password to the authentication server, and the authentication server does the authentication of the VPN user credentials.



Small Company Using Extended Authentication

CHAPTER 19

Configuring Managed VPN Tunnels

WatchGuard® System Manager supplies speed and reliability when you create IPSec VPN tunnels through the drag-and-drop procedure, an automatic wizard, and the use of templates. You can make IPSec tunnels that use authentication and encryption in minutes. You can be sure that these tunnels operate with other tunnels and security policies. From the same interface, you can control and monitor the VPN tunnels.

WatchGuard System Manager also allows you to safely manage Firebox® X Edge devices from a remote location. For more information, see the "Managing the Firebox X Edge and Firebox SOHO6" chapter.

Steps in making VPNs

- Configure a WatchGuard Management Server and Certificate Authority (CA)
- Add Fireboxes or Firebox X Edge or SOHO devices to the Management Server
- (Dynamic devices only) Configure the Firebox as a managed client
- Make policy templates to configure which networks can connect through VPN tunnels
- Make security templates to set the encryption type and authentication type
- Make tunnels between the devices

Configuring a Firebox as a Managed Firebox Client

To allow WatchGuard® System Manager to manage a Firebox®, Edge, or SOHO with a dynamic IP address, you must enable it as a managed Firebox client. For instructions on how to enable a Firebox as a managed client, see Chapter 16 "Using the Management Server."

Adding Policy Templates

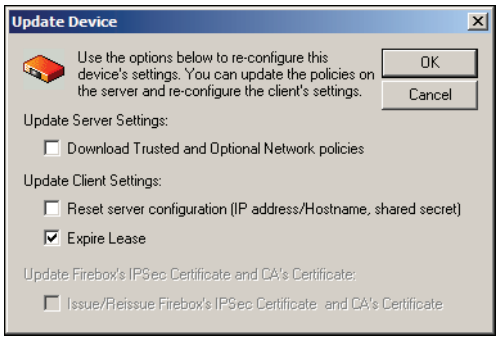
For a VPN, you can configure (and put a limit to) the networks that have access through the tunnel. You can make a VPN between hosts or networks. To configure the networks that are available through a given VPN device, you make policy templates. By default, WatchGuard® System Manager (WSM) adds

and applies a network policy template that gives access to the network behind the VPN device, if the device has a static IP address.

Get the current templates from a device

Before you add more policy templates, get the current templates from the device. This is most important for dynamic devices because the Firebox® automatically adds a network policy template for static devices. Before you update a device, make sure that it is configured as a managed Firebox client.

1 In WatchGuard System Manager on the **Device Management** tab, select a managed client, and then click **Edit > Update Device**.
The Update Device dialog box appears.


Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

2 Select the **Download Trusted and Optional Network Policies** check box.

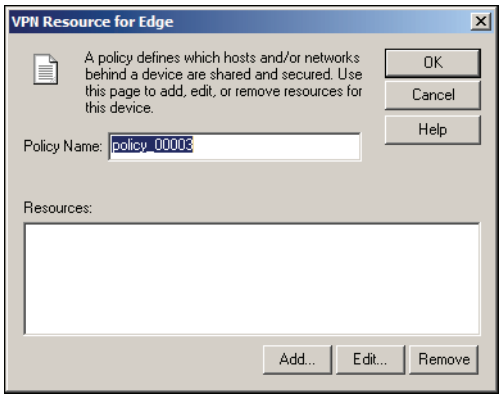
3 Click **OK**.

Make a new policy template

To make a policy template, on the **Device Management** tab:

1 Select the device for which you want to configure a policy template.

2 Right-click and select **Insert VPN Resource** or click the Insert VPN Resource icon.
The VPN Resource dialog box for that device appears.



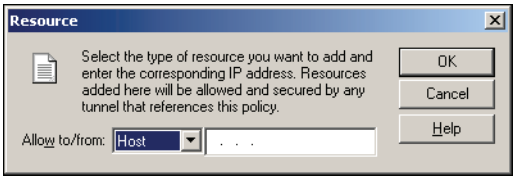
3 In the **Policy Name** box, type the policy name you want.

4 Add, edit, or delete resources from the tunnel policy. Click **Add** to add an IP address or a network address to the tunnel policy. Click **Edit** to edit a resource that you have selected in the list. Select a resource in the **Resources** list and click **Remove** to delete a resource.

5 Click **OK**.
The policy template is configured and is available in the VPN configuration area.

Adding resources to a policy template

1 From the **VPN Resource** dialog box, click **Add**.
The Resource dialog box appears.


Resource
Select the type of resource you want to add and enter the corresponding IP address. Resources added here will be allowed and secured by any tunnel that references this policy.
OK
Cancel
Help
Allow to/from:
Host

2 From the **Allow to/from** drop-down list, select the resource type, and then type the IP address or network address in the adjacent address box.

3 Click **OK**.

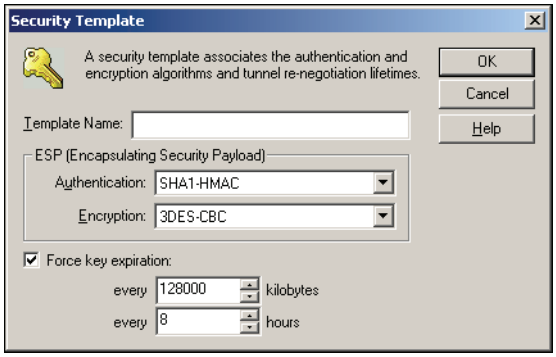
Adding Security Templates

A security template gives the encryption type and authentication type for a tunnel.

Default security templates are supplied for the available encryption types. You can also make new templates. Security templates make it easy to set the encryption type and authentication type with the tunnel from the Configuration wizard.

To make a policy template, on the **Device Management** tab:

1 Right-click in the window, and select **Insert Security Template** or click the Insert Security Template icon (shown at the left side).
The Security Template dialog box appears.



2 In the **Template Name** box, type the template name you want to use. From the **Authentication** and **Encryption** drop-down lists, select the authentication method and encryption method.

3 To set the end date for a key, select the **Force key expiration** check box, and then select the kilobytes or hours until the expiration.
If you give two values, the key stops at the event that comes first.

The security template is configured. You can select it in the VPN wizard when you make a VPN tunnel with that device.

4 Click **OK**.

Making Tunnels Between Devices

You can configure a tunnel with the drag-and-drop procedure or the Add VPN wizard.

Using the drag-and-drop procedure

Dynamic Fireboxes and Firebox® X Edge or SOHO devices must have networks that are configured before you can use this procedure. You must also get the policies from any new dynamic devices before you configure drag-and-drop tunnels (use the procedure "Get the current templates from a device" on page 238 to do this).

On the **Device Management** tab:

1 On one of the tunnel endpoints, click the device name. Drag-and-drop the name to the device name at the other tunnel endpoint.
The Add VPN wizard starts.

2 Click **Next**.

3 The gateway devices screen shows the two endpoint devices you selected with drag-and-drop, and the policy templates that the tunnel uses. If the endpoints are not shown, select them on this screen.

4 From the drop-down list, select a policy template for each device.
The policy template configures the resources available through the tunnel. Resources can be a network or a host.
The drop-down list shows the policy templates that you added to WatchGuard System Manager. If a VPN endpoint device has a static IP address, the Management Server automatically creates a default policy template for the device that includes all trusted networks. If the trusted network behind the device has many routed or secondary networks configured, some users prefer to create a custom template to restrict the resources available through the VPN tunnel.

5 Click **Next**.
The wizard shows the Security Policy dialog box.

6 Select the security template applicable for the type of security and type of authentication to use for this tunnel.
The list shows the templates you added to the Management Server.

7 Click **Next**.
The wizard shows the configuration.

8 Select the **Restart devices now to download VPN configuration** check box. Click **Finish** to start the devices again and deploy the VPN tunnel.

Using the Add VPN wizard without drag-and-drop

To use the Add VPN wizard to create tunnels:

1 From the **Device Management** tab, select **Edit > Create a new VPN** or click the Create New VPN icon.
This starts the Add VPN wizard.

2 Click **Next**.
The wizard shows two lists that each show all the devices registered in the Management Server.
3 Select a device from each list box to be the endpoints of the tunnel you make.
4 Select the policy templates for the end of the tunnel of each device.
The list shows the templates added to the Management Server.
5 Click **Next**.
The wizard shows the Security Template dialog box.
6 Select the applicable security template for this VPN and click **Next**.
The wizard shows the configuration.
7 Select the **Restart devices now to download VPN configuration** check box. Click **Finish** to start the devices again and deploy the VPN tunnel.

Editing a Tunnel

You can see all your tunnels on the **Device Management** tab of WatchGuard® System Manager (WSM). WSM lets you change the tunnel name, security template, endpoints, and the policy you use.

1 On the **Device Management** tab, expand the tree to see the device and its policy to change.
2 Select the tunnel you want to change.
3 Right-click and select **Properties**.
The Tunnel Properties dialog box appears.
4 Make the changes you want to the tunnel.
5 Click **OK** to save the changes.
When the tunnel is renegotiated, the changes are applied.

Removing Tunnels and Devices

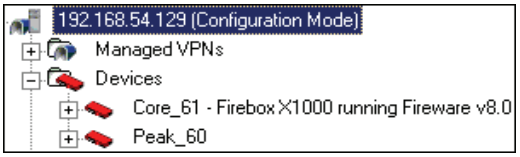
To remove a device from WatchGuard® System Manager (WSM), you must first remove the tunnels for which that device is an endpoint.

Removing a tunnel

1 From WSM, click the **Device Management** tab.
2 Expand the **Managed VPNs** folder to show the tunnel you want to remove.
3 Right-click the tunnel.
4 Select **Remove**. Click **Yes** to confirm
5 You may have to restart the devices that use the tunnel you want to remove. Click **Yes**.

Removing a device

1 From System Manager, click the **Device Status** or **Device Management** tab.
The Device Status tab (left side figure below) or the Device Management tab (right side figure below) appears.



2 If you use the **Device Management** tab, expand the **Devices** folder to show the device to remove.

3 Right-click the device.

4 Select **Remove**. Click **Yes**.

CHAPTER 20

Configuring BOVPN with Manual IPSec

You use Branch Office VPN (BOVPN) with manual IPSec to make encrypted tunnels between a Firebox® and an IPSec-compliant security device. This device can protect a branch office or a different remote location. BOVPN with manual IPSec can use different encryption methods: DES (56-bit), 3DES (168-bit), AES 128, AES 192, and AES 256.

Before You Start

You must have this information to use BOVPN with manual IPSec:

- Policy endpoints — IP addresses of hosts or networks that are accessible on the tunnel.
- Encryption method — the two ends of the tunnel must use the same encryption method.
- Authentication method — the two ends of the tunnel must use the same authentication method.

Configuring a Gateway

A gateway is a connection point for one or more tunnels. The connection method that the gateway uses to make a tunnel is the method you must use at the other end of the tunnel. The ISAKMP (Internet Security Association and Key Management Protocol) is one example.

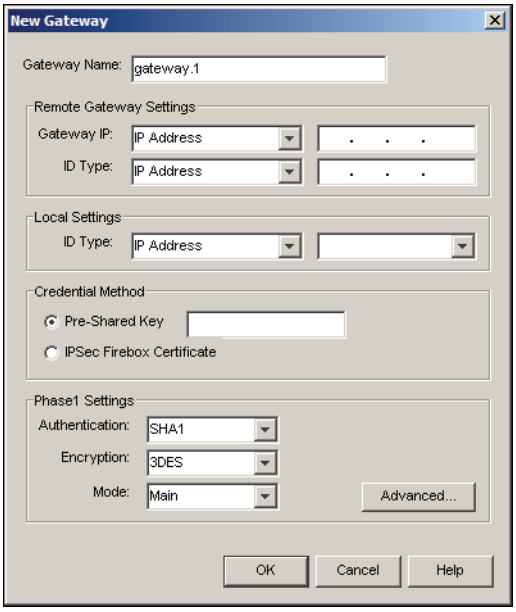
Adding a gateway

To start IPSec tunnel negotiation, one peer must connect to the other. You can use an IP address or a DNS name to connect the peers. If one peer has a dynamic IP address, select **Any** for the remote Gateway IP address.

To configure this, set the ID type of the remote gateway to **Domain Name** or **User Domain Name**. Set the peer name to the fully qualified domain name. Make sure the Firebox® is configured with DNS servers that can resolve the domain name.

1 From Policy Manager, click **VPN > Branch Office Gateways**.
The Gateways dialog box appears.

2 To add a gateway, click **Add**.
The New Gateway dialog box appears.



3 In the **Gateway Name** text box, type the gateway name.
This name identifies the gateway only in Policy Manager for this Firebox.

4 From the **Gateway IP** drop-down list, select **IP Address** or **Any**.
If the remote gateway address is a static IP address, type it in the adjacent address box. If the remote VPN endpoint has a dynamic IP address, select Any.

5 From the **Remote Gateway Settings ID Type** drop-down list, select **IP Address**, **Domain Name**, **User Domain Name**, or **X.500 Name**.
If the remote VPN endpoint uses DHCP or PPPoE to get its external IP address, set the ID type of the remote gateway to Domain Name. Set the peer name field to the fully qualified domain name of the remote VPN endpoint. The Firebox uses IP address and Domain Name to find the VPN endpoint. Make sure the DNS server used by the Firebox can identify the name.

6 Configure the Local Settings. In the local **ID Type** drop-down list, select **IP address, Domain Name**, or **User Domain Name**. If you select **IP address**, you can select the IP address from the adjacent drop-down list. All configured Firebox interface IP addresses are shown.

7 Click **Pre-Shared Key** or **Firebox Certificate** to identify the authentication procedure to use. If you select **Pre-Shared Key**, type the shared key.
You must use the same shared key on the remote device. This shared key must use only standard ASCII characters.

Note

You must start the Certificate Authority if you select certificate-based authentication. For information on this, see the Certificate Authority chapter earlier in this manual. Also, if you use certificates you must use the WatchGuard® Log Server for log messages. We do not support third-party certificates.

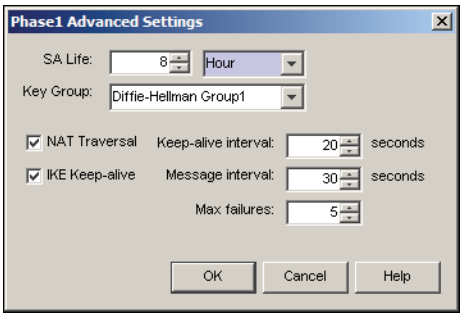
8 You can use the default Phase 1 settings, or you can change the settings If you want to use the default setttings, you can move ahead to step 19.
Phase 1 applies to the initial phase of the IKE negotiation. It contains authentication, session negotiation, and key change information.

9 From the **Authentication** drop-down list, select **SHA1** or **MD5** as the type of authentication.

10 From the **Encryption** drop-down list, select, **None**, **DES** or **3DES** as the type of encryption.

11 From the **Mode** drop-down list, select **Main** or **Aggressive**.
Main Mode does not identify the VPN endpoints during negotiation, and is more secure than Aggressive Mode. Main Mode also supports Diffie-Hellman group 2. Main Mode is slower than Aggressive Mode because Main Mode must send more messages between endpoints.

12 If you want to change the Diffie-Hellman group settings and other advanced Phase 1 settings, click **Advanced**.
The Phase1 Advanced Settings dialog box appears.



13 To change the SA (security association) life, type a number in the **SA Life** field, and select **Hour** or **Minute** from the drop-down list.

14 From the **Key Group** drop-down list, select the Diffie-Hellman group you want. WatchGuard supports groups 1 and 2.
Diffie-Hellman groups are sets of properties used to safely negotiate secret keys across a public medium. Group 2 is more secure than group 1, but uses more time to make the keys.

15 If you want to use NAT devices through the tunnel, select the **NAT Traversal** check box. To set the **Keep-alive interval**, type the number of seconds or use the value control to select the number of seconds you want.
NAT Traversal, or UDP Encapsulation, allows traffic to get to the correct destinations. Enable NAT traversal when you want to build a BOVPN tunnel between the Firebox and another device that is behind a NAT device.

16 To have the Firebox send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box. To set the **Message Interval**, type the number of seconds or use the value control to select the number of seconds you want.

17 To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.

18 When you complete the advanced configuration, click **OK**.

19 Click **OK** to save the gateway.

20 Click **Close** to close the **Gateways** dialog box.

Editing and deleting gateways

To change a gateway, select **VPN > Branch Office Gateways**. Or, right-click on a tunnel icon in the **BOVPN** tab of Policy Manager, and select **Gateway Property**.

1 Select the gateway you want and click **Edit**.
The Edit Gateway dialog box appears.

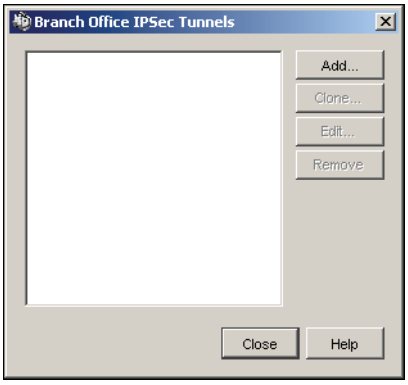
2 Make the changes and click **OK**.

To delete a gateway, select the gateway and click **Remove**.

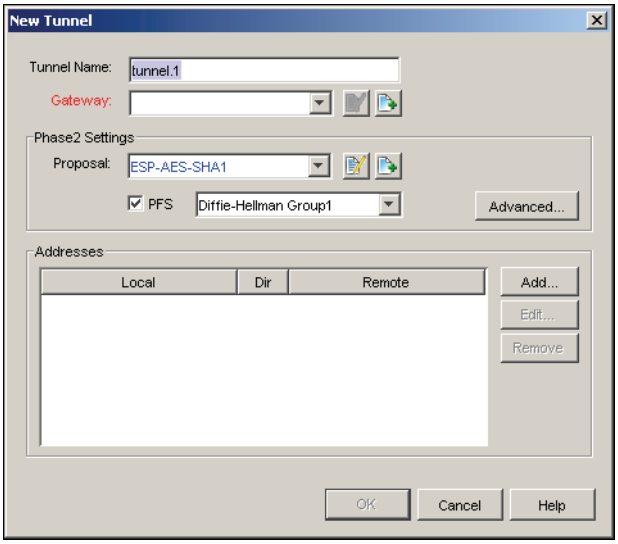
Making a Manual Tunnel

Use this method to configure a manual tunnel that uses a gateway with the ISAKMP (Internet Security Association and Key Management Protocol) key negotiation type. ISAKMP is a protocol that authenticates network traffic between two devices. This procedure includes the information on how the devices control security, which includes encryption. The procedure also includes the information used to make the keys that are used to change the encrypted data into text.

1 From Policy Manager, select **VPN > Branch Office Tunnels**.
The Branch Office IPSec Tunnels dialog box appears.



2 Click **Add**.
The New Tunnel dialog box appears.



3 In the **Tunnel Name** box, type the tunnel name you want.

4 From the **Gateway** drop-down list, select a remote gateway to connect with this tunnel. The gateways you add to your configuration appear in this drop-down list.

To edit a gateway, select the name and click the **Edit** button. To create a new Gateway, click the **New** button.

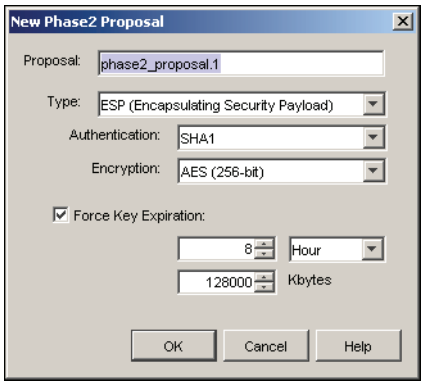
Edit

New

5 From the **Proposal** drop-down list, select the IKE Phase 2 proposal for your tunnel. The drop-down list contains predefined phase 2 security proposals. If you want to use the default phase 2 proposal, and not create or edit a phase 2 proposal, go to step 14.

You can edit any phase 2 proposal that you create, but you cannot edit a predefined proposal. You must add a new one. To edit a phase 2 proposal that you create, select the proposal name and click the **Edit** button. To create a new proposal, click the **New** button.

The Phase2 Proposal dialog box appears.



6 Type a name for the new proposal.

7 From the **Type** drop-down list, select **ESP** or **AH** as the proposal method.
ESP is authentication with encryption. AH is authentication only. Also, ESP authentication does not include the IP header, while AH does. The use of AH is rare.

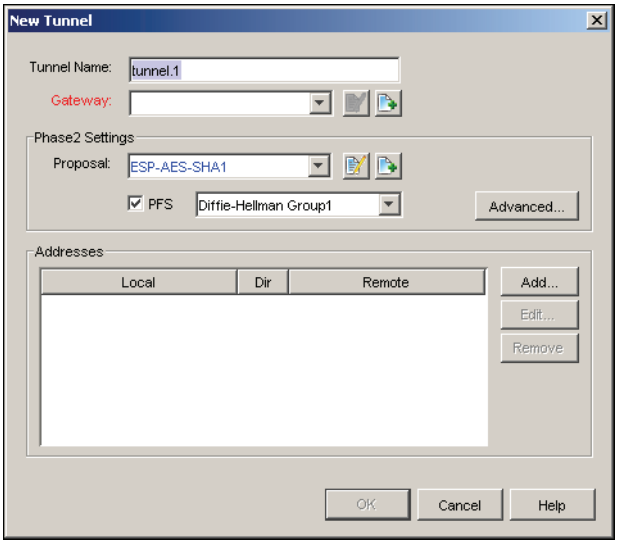
8 From the **Authentication** drop-down list, select **SHA1**, **MD5**, or **None** for the authentication method.

9 (ESP only) From the **Encryption** drop-down list, select the encryption method.
The options are DES, 3DES, and AES 128, 192, or 256 bit which appear in the list from the most simple and least secure to most complex and most secure.

10 You can make the key expire after a quantity of time or a quantity of traffic. To enable key expiration, select the **Force Key Expiration** check box.

11 Enter a quantity of time and a number of bytes after which the key expires.

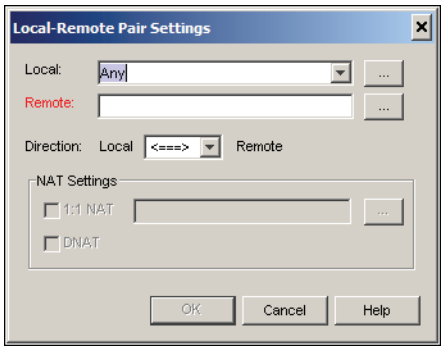
12 Click **OK** to close the **Phase2 Proposal** dialog box.



13 Select the **PFS** check box to enable Perfect Forward Secrecy (PFS). If you enable PFS, select the Diffie-Hellman group.
Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure. Diffie-Hellman Group 1 uses a 768-bit group to create the new key exchange, and Diffie-Hellman Group 2 uses a 1024-bit group.

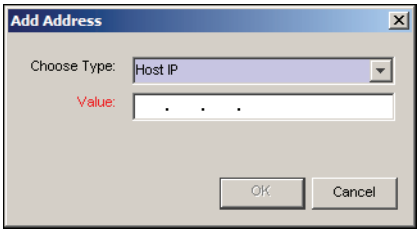
14 Click **Advanced** to configure advanced settings. Use the **Phase2 Advanced Settings** dialog box to configure the tunnel to use Any for the policy or for the address. Click **OK** when you are done.
If "Use Any for Service" is not selected, a security association (SA) is created for each set of port/protocol pairs defined in each policy that is used. This creates a different VPN tunnel for each policy. If "Use Any for Address" is not selected, a security association (SA) is created based on the tunnel routes (the local-remote pairs).

15 In the **Addresses** block of the **New Tunnel** dialog box, click **Add** to add a pair of addresses that use the tunnel.
The Local-Remote Pair Settings dialog box appears.



16 From the **Local** drop-down list, select the local address you want.
You can also click the button adjacent to the Local drop-down list to use an IP address, network address, or a range of IP addresses.

17 In the **Remote** box, type the remote network address. Click the button adjacent to the **Remote** box to open the **Add Address** dialog box.



18 From the **Choose Type** drop-down list, select the type of address you want to use.
Select **Host IP** (one IP address), **Network IP** (a network IP address with the mask in slash notation), or **Host Range** (a range of IP addresses).

19 In the **Value** text box, type an IP address or network address.

20 Click **OK**.
The Add Address dialog box closes.

21 From the **Direction** drop-down list, select the direction for tunnel. The tunnel direction decides which endpoint of the VPN tunnel can start a VPN connection through the tunnel.

22 You can enable NAT for the tunnel. Select the **1:1 NAT** check box or the **DNAT** check box.
The options that you can select for NAT are different for different types of addresses and different tunnel directions. For 1:1 NAT, type the address to change with NAT in the field.
Dynamic NAT is also available through the VPN. You must set a unidirectional tunnel from LAN1 to LAN2 where you want all LAN1 servers to connect to LAN2 servers but appear as only one IP address on LAN2. For information on how to do this, see "Setting up Outgoing Dynamic NAT through a BOVPN Tunnel" on page 250.

23 After you configure the pair, click **OK**.

24 When you complete the tunnel configuration, click **OK**.

Editing and deleting a tunnel

To change a tunnel, select **VPN > Branch Office Tunnels**. Or, right-click on a tunnel icon in the **Branch Office VPN** tab of Policy Manager, and select **Tunnel Property**.

1 Select the tunnel and click **Edit**.
The Edit Tunnel dialog box appears.

2 Make the changes and click **OK**.

To delete a tunnel from the **Branch Office IPSec Tunnels** dialog box, select the tunnel and click **Remove**.

Making a Tunnel Policy

Tunnel policies are sets of rules that apply to tunnel connections.

By default, the "Any" policy is created when a VPN tunnel is created. This policy allows all traffic to use the tunnel. You can delete this policy. Then, you can create a custom VPN policy to allow specified ports or use a proxy.

1 From Policy Manager, click the **Branch Office VPN** tab.

2 From the **Show** menu, select the tunnel to which you want to add policies.

3 Right-click in Policy Manager and select **Add Policy.**

If you have not selected a BOVPN tunnel from the Show menu, a dialog box appears with a prompt for you to select a tunnel. Select the tunnel and click OK.

4 Configure policies. For more information, see "Creating Policies for your Network" on page 65.

Address information for BOVPN policies is different from standard Firebox policies. You configure the addresses with the Local-Remote Pairs dialog box.

Allow VPN connections for specified policies

To let traffic through from VPN connections only for specified policies, add and configure each policy. It can be necessary to delete the "Any" policy to create the necessary restrictions.

Setting up Outgoing Dynamic NAT through a BOVPN Tunnel

You can use dynamic NAT through BOVPN tunnels. Dynamic NAT acts as unidirectional NAT, and keeps the VPN tunnel open in one direction only. This can be helpful when you make a BOVPN to remote site where all VPN traffic comes from one public IP address.

For example, suppose you want to create a BOVPN tunnel to a business partner so you can get access to their database server, but you do not want this company to get access to any of your resources. Your business partner wants to allow you access, but only from a single IP address so they can monitor the connection.

You must have the external IP address and the trusted network address of each VPN endpoint to do this procedure.

1 From Policy Manager at your site, select **VPN > Branch Office Tunnels**. Select **Add** to add a new BOVPN tunnel.

2 Give the BOVPN tunnel a name.

3 Select the New Phase 2 Proposal icon (button at the far right of the **Gateway** field).

The New Gateway dialog box appears

4 Create a new gateway, as described in the beginning of step 3 of "Adding a gateway" on page 243.

5 Click **OK** to return to the **New Tunnel** dialog box.

6 Click **Advanced**. Clear all check boxes. Click **OK**.

If you do not change these Phase 2 Advanced Settings, your BOVPN tunnel will not negotiate correctly. Without this change, the second VPN endpoint will look for the first endpoint's trusted network instead of its external interface after you enable dynamic NAT.

7 Click **Add** to add a tunnel policy. Use the procedure that starts with "From the **Local** drop-down list" on page 249 to do this. Make sure you select the **DNAT** check box.

8 Click **OK**. Save these changes to the Firebox®.

9 From Policy Manager at the remote site, select **VPN > Branch Office Tunnels**. Select **Add** to add a new BOVPN tunnel.

10 Do steps 2 – 8 at the remote site, but do not select the **DNAT** check box.

When the Firebox at the remote site restarts, the two Firebox devices negotiate a VPN tunnel. Your Firebox applies dynamic NAT to all traffic destined for the trusted network of the remote site. When this traffic reaches the remote site, it arrives as traffic that originated on your external interface.

CHAPTER 21

Managing the Firebox X Edge and Firebox SOHO

WatchGuard® System Manager includes a number of features specifically for Firebox® X Edge device management. You can easily manage many Firebox X Edge devices, make changes to the security policy for more than one Firebox X Edge device at one time, and still have individual control over the configuration of each Firebox X Edge device. With a Management Server, you can:

- Create Edge Configuration Templates for a group of Firebox X Edge devices. You create a configuration template on the Management Server, and install it on many Firebox X Edge devices. To do this, select an Edge Configuration Template from the list, or drag the Firebox X Edge devices on to the template. If you make a change to the policy, the policy is automatically updated on all subscribed Firebox X Edge devices.
- Manage network settings for a group of Firebox X Edge devices, all from WatchGuard System Manager.
- Configure factory default Firebox X Edge devices with the Quick Setup Wizard, and prepare the devices for management with the Management Server. You can then import the devices into the Management Server in one step.
- See settings for more than one Firebox X Edge device in a simple layout, and easily change settings.
- See all VPN tunnels for a Firebox X Edge.
- Manage Firebox X Edge firmware updates. With a Management Server, firmware updates can be scheduled and installed by the Management Server.

You can also manage Firebox SOHO 6 and SOHO 5 devices from WatchGuard System Manager. You cannot create configuration templates for the Firebox SOHO, or edit the network configuration with WatchGuard System Manager. You can:

- See settings for a group of Firebox SOHO devices in a simple layout.
- See all VPN tunnels for a Firebox SOHO.

Note

This chapter describes how to use WatchGuard System Manager to manage Firebox X Edge devices. For detailed information on configuring the Firebox X Edge, see the *Firebox X Edge User Guide*.

Working with Devices on a Management Server

You can use WatchGuard® System Manager with a WatchGuard Management Server to configure and manage many Firebox® X Edge devices, and to manage many Firebox SOHO devices.

Each Firebox X Edge and SOHO must be configured for management by the Management Server. Then you **Insert** or **Import** the devices to the Management Server.

You can **Import** one or more Firebox X Edge devices that have already been configured with the Quick Setup Wizard into the Management Server. This is the fastest procedure to add a group of Firebox X Edge devices to the Management Server.

You can **Insert** a Firebox X Edge device that is already configured or installed using the Add Device Wizard. You must configure values to identify the device to the Management Server. You can insert only one device at a time.

- For a new or factory default Firebox X Edge device, configure the device with the procedure "Preparing a new or factory default Firebox X Edge for management" on page 254, then import the device with the procedure "Importing Firebox X Edge devices into a Management Server" on page 255.
- For a Firebox X Edge that is already installed, configure the device for management with the procedure "Preparing an installed Firebox X Edge for management" on page 255, and insert the device into the Management Server using the procedure "Adding Firebox X Edge and SOHO 6 devices to a Management Server" on page 257.

After you configure a Firebox X Edge for management by a Management Server, you must reset it to factory defaults to restore it to its original state.

Note

The Management Server connects to managed Firebox X Edge devices on TCP port 4109. Make sure that you have a policy to allow traffic from managed Edge devices on TCP port 4109 on the gateway Firebox or other firewall that protects the Management Server from the Internet.

Preparing a new or factory default Firebox X Edge for management

To prepare a new or factory default Firebox X Edge for management with a Management Server, you must be able to physically connect the Firebox X Edge to an Ethernet interface on your computer.

To prepare the Firebox X Edge:

1. Start WatchGuard System Manager and select **Tools > Quick Setup Wizard**.
   The Quick Setup Wizard starts.
2. Read the Welcome page and click **Next**.
3. Select **Firebox X Edge** as the type of Firebox and click **Next**.
4. Connect the network interface on your computer to any LAN port on the Firebox X Edge, and click **Next**.

   Use one of the green Ethernet cables included with the Firebox X Edge. (If there is no green cable included with your Firebox X Edge, try the red cable.) Look at the light on the Edge front panel that has a number corresponding to the number of the Ethernet port you connected the cable to on the back of the Edge. If the light comes on, there is a good physical connection. If the light does not come on, use a different cable. It is possible the cable is bad or that it is a crossover cable. A straight-through Ethernet cable is usually required, but the important thing is that you see the link light come on.
5. Use the instructions on the subsequent page of the wizard to start the Firebox X Edge in Safe Mode.
6. Use the instructions on the wizard page, and click **Next**.

7 Use the instructions on the **Wait for the Firebox** and **The Wizard found this Firebox** pages. Click **Next** after each page.

8 Accept the License Agreement and click **Next**.

9 Configure the external (WAN 1) interface of the Firebox X Edge. Select **DHCP**, **PPPoE**, or **Static IP addressing**, and click **Next**. (For detailed information on how to configure the Edge interfaces, see the *Firebox X Edge User Guide*.)

10 Click **Next** after you configure the interface.

11 Configure the Edge internal interface and click **Next**.

12 Create a status passphrase and a configuration passphrase for your Edge and click **Next**.
You must type each passphrase two times. This is the passphrase that is used by WatchGuard System Manager to connect to and configure the device.

13 Type a user name and passphrase for the device, and click **Next**.
You must type the passphrase two times. This is the user name and passphrase that you can use to connect to and configure the device with a web browser.

14 Select the time zone settings and click **Next**.

15 Configure the Management Server settings. Type the IP address of the gateway Firebox that protects the Management Server, the name to identify the Firebox in the Management Server interface, and the shared key. Click **Next**.
The shared key is used by the Management Server to create VPN tunnels between Fireboxes. You do not have to remember this key.

16 Review the configuration for the Edge and click **Next**.

17 To set up another Edge, select the check box. Click **Finish**.
If you select this check box, the Quick Setup Wizard populates the fields with the same values as this configuration, so you can easily set up similar Edge devices.

Importing Firebox X Edge devices into a Management Server

Firebox X Edge devices that are configured with the Quick Setup Wizard can be imported into the Management Server.

1 Start WatchGuard System Manager, and connect to the Management Server for which you configured Edge devices.

2 Select **File > Import Device**.
The Import Device dialog box appears.

3 Select the check boxes in front of each Edge you want to import. Click **Import**.

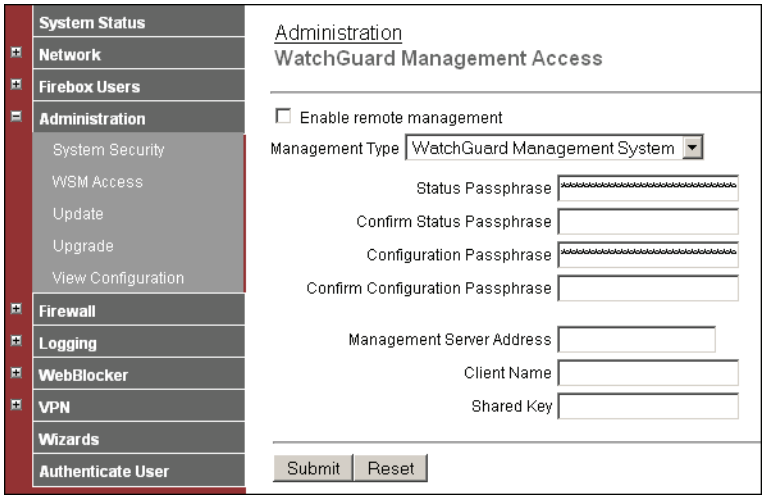
The Firebox X Edge devices are imported into the Management Server. The devices appear in the **Imported Devices** folder for the Management Server.

Preparing an installed Firebox X Edge for management

1 Start your web browser. Type the IP address of the Firebox X Edge.

2 Type a user name and passphrase to log on to the Edge, if required.

3 Click **Administration**. Click **WSM Access**.
The WatchGuard Management Access page appears.



4 Select the **Enable Remote Management** check box.

5 From the **Management Type** drop-down list, select **WatchGuard Management System**.

6 Type the status passphrase for WatchGuard management. Type the status passphrase again to confirm the passphrase.
This is a passphrase you create that the WatchGuard Management Server uses to connect to this device in read-only mode.

7 Type the configuration passphrase for WatchGuard Management. Type the configuration passphrase again to confirm the passphrase.
This is a passphrase you create that the WatchGuard Management Server uses to configure this device.

8 (Optional, but recommended) Type the Management Server address. This is the public IP address of the Firebox that the Management Server is behind.
If you do not type the Management Server address, the connection between the Firebox X Edge and the Management Server must be started from the Management Server.

9 (Optional) Type the client name.
This is the name that the Management Server uses to identify the Edge.

10 (Optional) Type the shared key, if one has been configured.

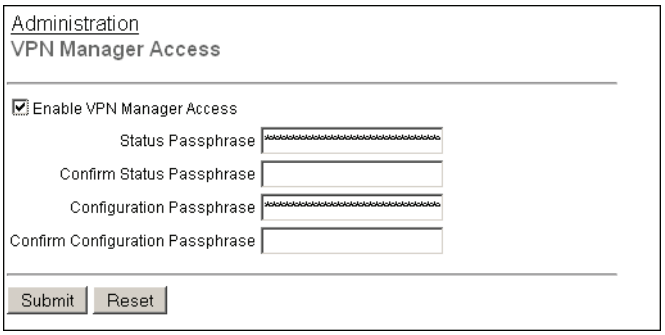
11 Click **Submit**.
The Edge is configured for management by the Management Server.

Preparing a Firebox SOHO 6 for management

1 Start your web browser. Type the IP address of the SOHO 6.

2 Type a user name and passphrase to log on to the SOHO 6, if required.

3 Below Administration, click **VPN Manager Access**.
The VPN Manager Access page appears.



4 Select the **Enable VPN Manager Access** check box.

5 Type the status passphrase for VPN Manager access. Type the status passphrase again to confirm the passphrase.

6 Type the configuration passphrase for VPN Manager access. Type the configuration passphrase again to confirm the passphrase.

7 Click **Submit**.
The SOHO 6 device is configured for management by the Management Server.

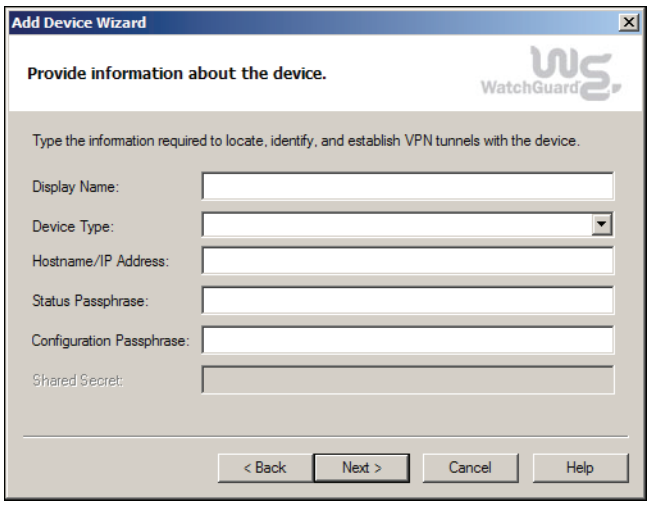
Adding Firebox X Edge and SOHO 6 devices to a Management Server

1 In WatchGuard System Manager, connect to the Management Server.
Select File > Connect to Server, or select either the Device Status or Device Management tab, right-click, and select Connect to > Server.

2 Click the **Device Management** tab.

3 Expand the **Devices** folder.
All devices managed by this Management Server are shown here.

4 Select **Edit > Insert Device**, or right-click in the left frame of this window and select **Insert Device**.
The Add Device Wizard starts. Click Next to see the first configuration screen.



5 Type a display name for the device.
This name cannot include any spaces or punctuation marks.

6 From the **Device Type** drop-down list, select the Firebox model.

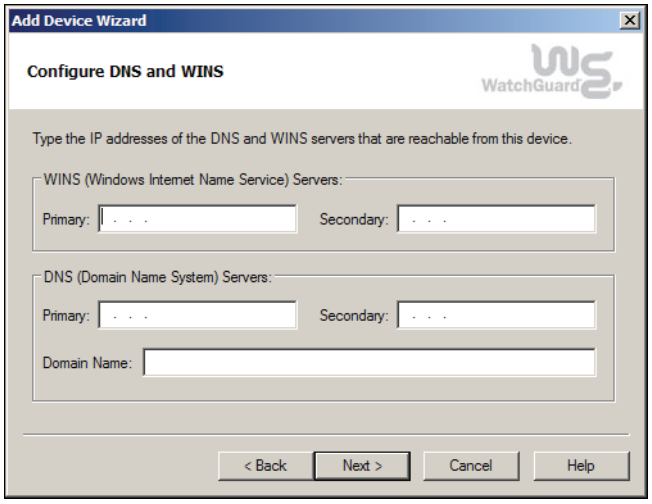
7 For devices that do not use a dynamic IP address, type the IP address or host name. For devices that use a dynamic IP address, type the Dynamic DNS service client name.

8 Type the status passphrase. This is the status passphrase for the Firebox X Edge or SOHO 6 that you configured when you set up VPN Manager access or WatchGuard Management access.

9 Type the configuration passphrase. This is the configuration passphrase for the Firebox X Edge or SOHO 6 that you configured when you set up VPN Manager access or WatchGuard Management access.

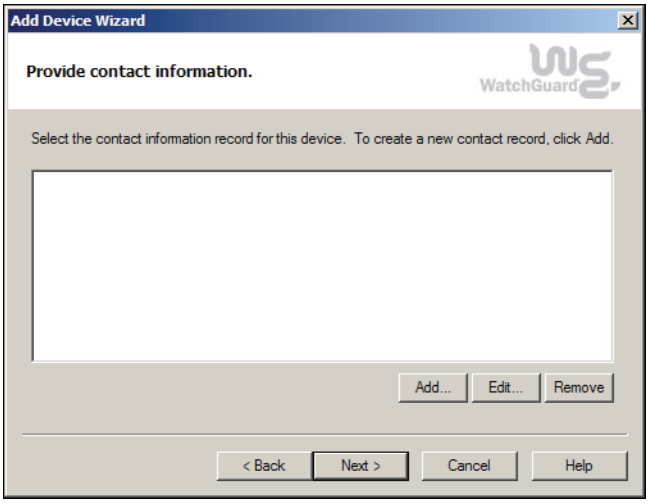
10 If the Firebox X Edge or SOHO 6 uses a dynamic IP address, type the Dynamic DNS client shared secret.

11 Click **Next**.
The Configure WINS and DNS screen appears.



12 Type primary and secondary addresses for the WINS and DNS servers this device uses, if any.

13 Type the domain name for this device, if any. Click **Next**.
The Provide Contact Information screen appears.



14 You can select an existing contact record for this device, or click **Add** to add a new contact record for this device. To delete an existing contact record, select it and click **Delete**.

15 Click **Next**. The Configure the Device screen appears. Click **Next** on this screen to configure the device with the new management settings and add it to the Management Server. If the device is already managed by another server, or configured for management by this server, a warning dialog box appears. Click **Yes** to continue.
You cannot configure Firebox SOHO devices with the Management Server.

16 Click **Close** to close the Add New Device wizard.

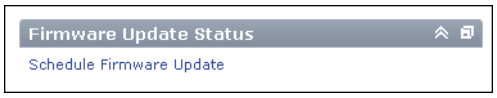
Scheduling Firebox X Edge Firmware Updates

Firebox® X Edge devices must have a firmware update to operate with the advanced features of the Management Server. In the future, more firmware updates could be required. These firmware updates are installed on the Management Server, and the Management Server loads them on the Edge devices. WatchGuard® System Manager can install firmware updates to a group of Edge devices easily. You can update firmware on groups of devices with one operation, either immediately or on a schedule.

You get firmware updates from LiveSecurity.

1 In the **Device Management** tab in WatchGuard System Manager, select the Management Server.
The Management Server settings page appears.

2 Scroll down to the **Firmware Update Status** section.
If there are scheduled firmware updates, they are shown here.



3 Click **Schedule Firmware Update**.
The Update Firmware wizard starts.

4 Read the Welcome screen and click **Next**.

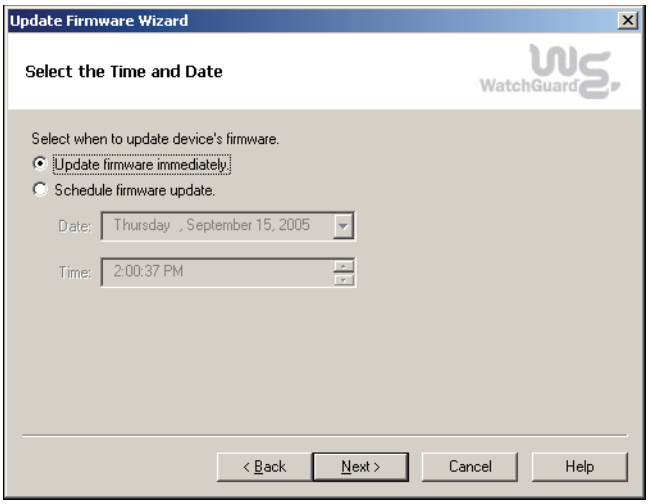
5 Select the device type from the list and click **Next**.

Note

In this version of WatchGuard System Manager, the only device type you can select is Firebox X Edge.

6 Select the check box in front of each Firebox X Edge that you want to update. Click **Next**.

7 Select the firmware version to use. Click **Next**.
The Select the Time and Date page appears.



8 To update firmware immediately, select **Update firmware immediately**. To schedule the update for a time in the future, select **Schedule firmware update**.

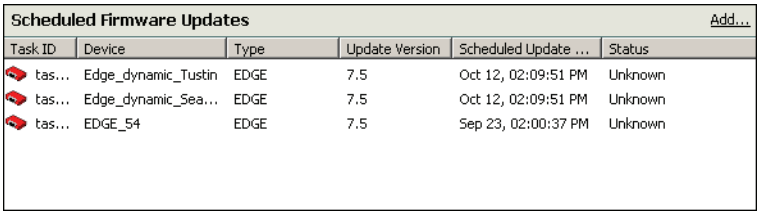
9 If you selected **Schedule firmware update**, select the date from the **Date** field, and set the time in the **Time** field.

10 Click **Next**.

11 Click **Next**. Click **Close**.
The Firmware is updated if you selected Update firmware immediately, or scheduled if you selected Schedule firmware update.

Viewing and deleting firmware updates

1 In the **Device Management** tab, click **Scheduled Firmware Updates** below the Management Server.
The Scheduled Firmware Updates page appears.



All scheduled firmware updates are shown. Firmware updates are shown separately for each device, even if more than one device is included in the same firmware update. For this reason, when you select a device, all devices included in that scheduled firmware update are also selected.

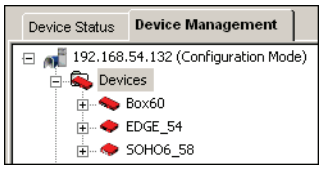
- To delete a scheduled firmware update, right-click a device and select **Remove task**.
All devices in that firmware update task are removed from the schedule.
- To add a scheduled firmware update, click **Add**.
The Update Firmware wizard starts.

Using the Firebox X Edge Management Page

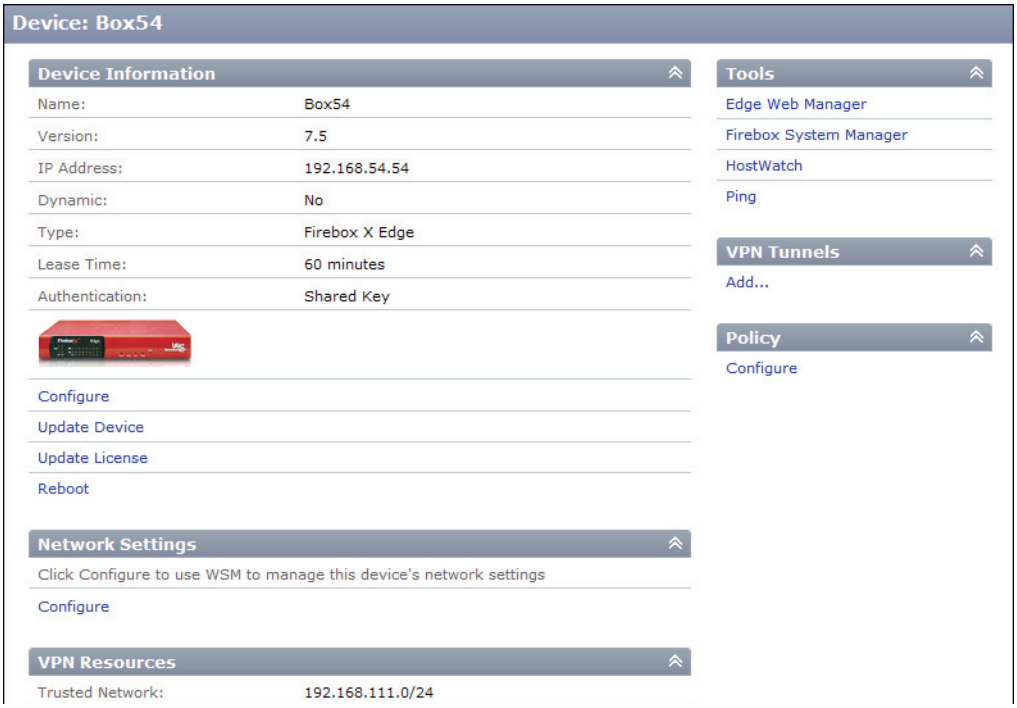
When the Firebox® X Edge is added to a Management Server, you can use the management page to configure settings on the device.

Viewing the Firebox X Edge management page

1 Expand **Devices** in the WatchGuard® System Manager **Device Management** tab.
A list of managed devices appears.

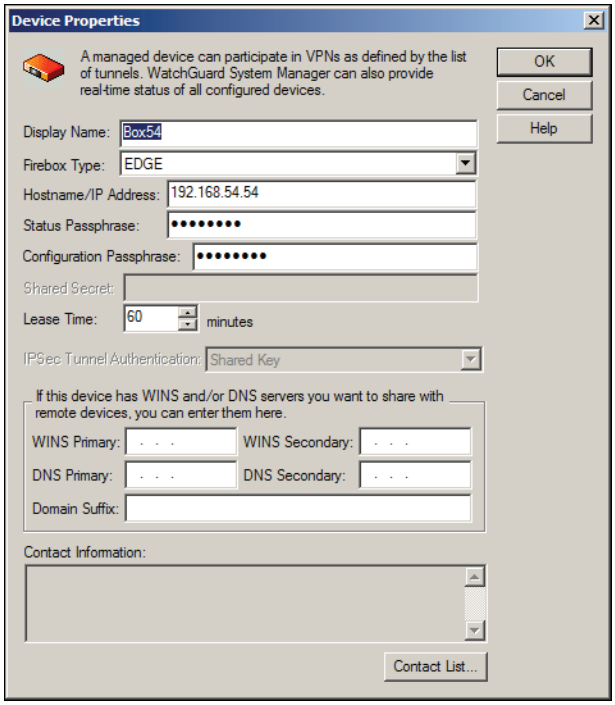


2 Select a Firebox X Edge. The management page for the device appears.



Configuring Firebox X Edge management properties

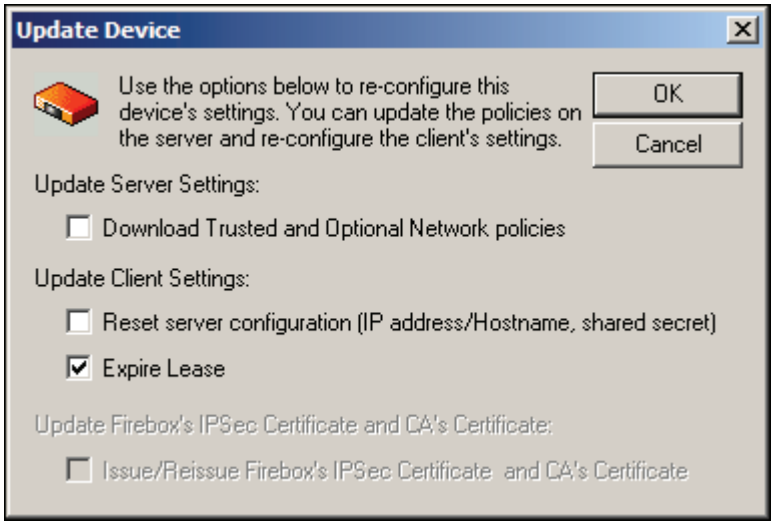
1 On the Firebox X Edge management page, click **Configure**.
The Device Properties dialog box appears.


Device Properties
A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.
OK
Cancel
Help
Display Name: Box54
Firebox Type: EDGE
Hostname/IP Address: 192.168.54.54
Status Passphrase:
Configuration Passphrase:
Shared Secret:
Lease Time: 60 minutes
IPSec Tunnel Authentication: Shared Key
If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.
WINS Primary:
WINS Secondary:
DNS Primary:
DNS Secondary:
Domain Suffix:
Contact Information:
Contact List...

2 Configure the management properties for the device. For information on individual fields in this dialog box, see the *Firebox X Edge User Guide*.

Updating the device

1 On the Firebox X Edge management page, click **Update Device**.
The Update Device dialog box appears.

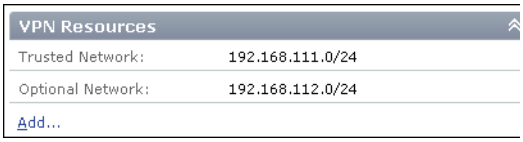

Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

2 You can use this dialog box to get the policies from the Firebox X Edge device, reset the Management Server configuration for the device, and expire the management lease. You can also use this dialog box to update the Firebox certificate and the CA certificate, if it has changed.

3 Click **OK**.

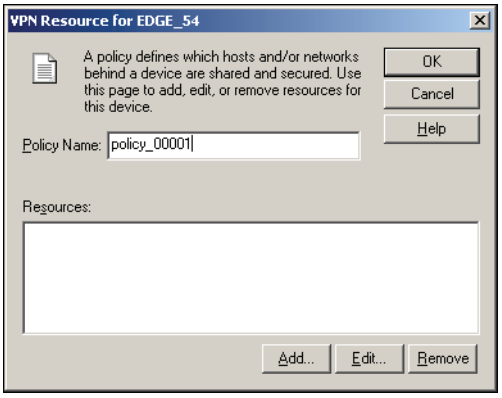
Adding a VPN Resource

1 On the Firebox X Edge management page, find the VPN Resources section.



The VPN resources for the device are shown.

2 Click **Add**.



3 Add, edit, or remove VPN resources.
A VPN resource is an IP address or network address to which VPN users can securely connect.

4 Click **OK**.
The new VPN resource appears on the list.

Starting Firebox X Edge tools

The management page allows you to start four tools for Firebox X Edge configuration and monitoring:

- Edge Web Manager. You can use Netscape 7.0 (or later), Internet Explorer 6.0 (or later), Mozilla Firefox 1.0 or later, or an equivalent browser.
- Firebox System Manager
- HostWatch
- Ping

To start any of these tools, click the link for the tool from the Tools section on the Firebox X Edge management page.

Adding a Firebox X Edge VPN Tunnel

The Firebox X Edge management page shows all tunnels that include the device in the Tunnels section. You can also add a VPN tunnel in this section.

1 On the Firebox X Edge management page, find the VPN Tunnels section.

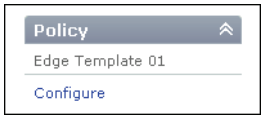
This section shows all tunnels in which this device is a VPN endpoint.

2 Click **Add** to add a new VPN tunnel.
The Add VPN wizard starts. Configure the VPN to match your VPN requirements.

For more information about the Add VPN Wizard, see the chapter "Configuring Managed VPN Tunnels".

Using the Firebox X Edge Policy section

This section shows the Edge Configuration Template to which this Firebox X Edge is subscribed. You can use the **Configure** link in this section to configure the Edge Configuration Template.

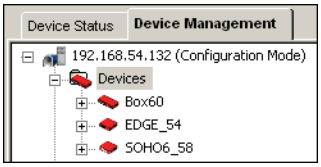


Using the Firebox SOHO 6 Management Page

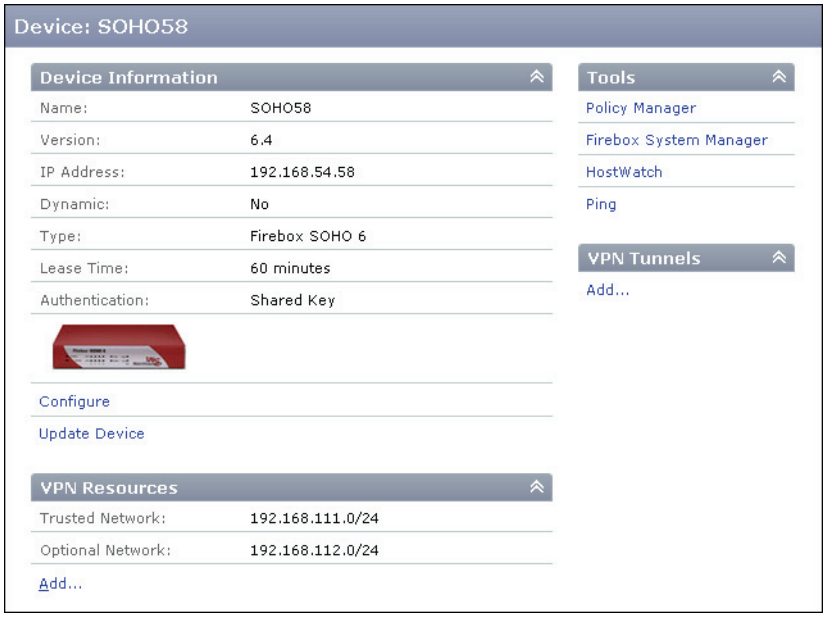
When the Firebox® SOHO 6 is added to a Management Server, you can use the management page to configure settings on the device.

Viewing the SOHO 6 management page

1 Expand **Devices** in the WatchGuard® System Manager **Device Management** tab.
A list of managed devices appears.

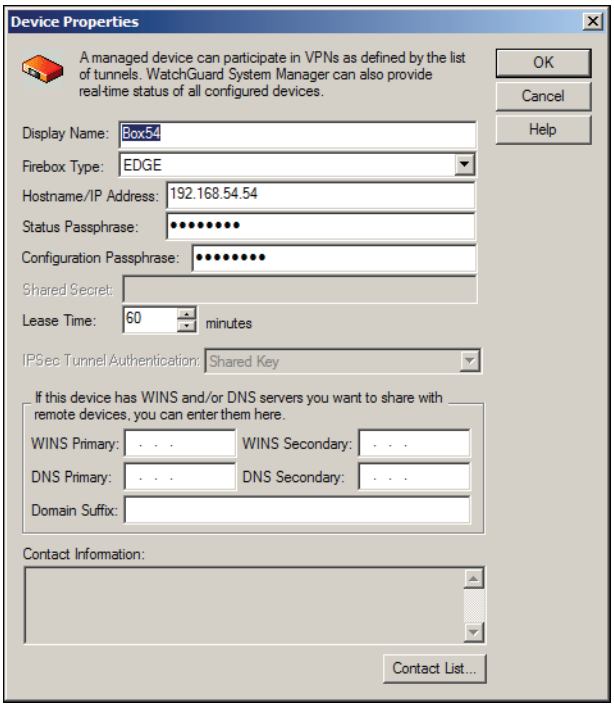


2 Select a Firebox SOHO 6. The management page for the device appears.



Configure Firebox SOHO 6 management properties

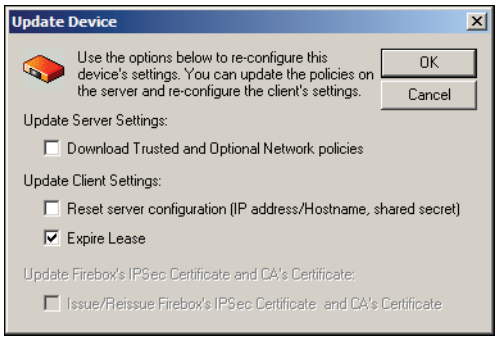
1 On the Firebox SOHO 6 management page, click **Configure**.
The Device Properties dialog box appears.


Device Properties
A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.
OK
Cancel
Help
Display Name: Box54
Firebox Type: EDGE
Hostname/IP Address: 192.168.54.54
Status Passphrase:
Configuration Passphrase:
Shared Secret:
Lease Time: 60 minutes
IPSec Tunnel Authentication: Shared Key
If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.
WINS Primary:
WINS Secondary:
DNS Primary:
DNS Secondary:
Domain Suffix:
Contact Information:
Contact List...

2 Configure the management properties for the device. For information on individual fields in this dialog box, see the *Firebox SOHO User Guide*.

Updating the device

1 On the Firebox SOHO 6 management page, click **Update Device**.
The Update Device dialog box appears.

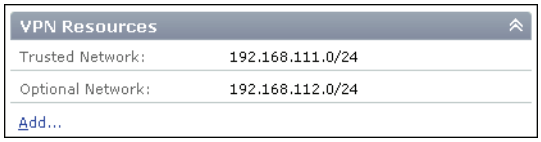

Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

2 You can use this dialog box to get the policies from the device, and to reset the Management Server configuration for the device, and expire the management lease. You can also use this dialog box to update the Firebox certificate and the CA certificate, if it has changed.

3 Click **OK**.

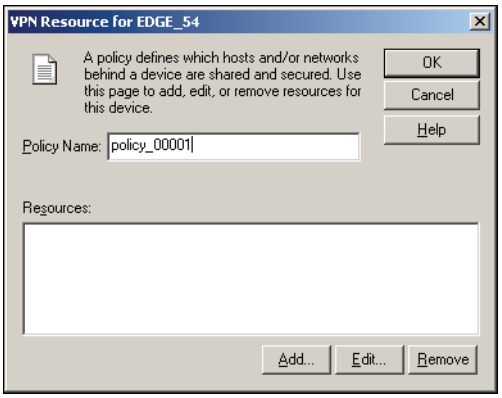
Adding a VPN Resource

1 On the Firebox SOHO 6 management page, find the VPN Resources section.



The VPN resources for the device are shown.

2 Click **Add**.


VPN Resource for EDGE_54
A policy defines which hosts and/or networks behind a device are shared and secured. Use this page to add, edit, or remove resources for this device.
OK
Cancel
Help
Policy Name: policy_00001
Resources:
Add...
Edit...
Remove

3 Add, edit, or remove VPN resources.
A VPN resource is an IP address or network address to which VPN users can securely connect.

4 Click **OK**.
The new VPN resource appears on the list.

Starting Firebox SOHO 6 tools

The management page allows you to start four tools for Firebox SOHO 6 configuration and monitoring:

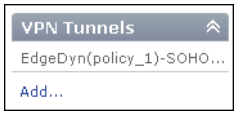
- Policy Manager (the SOHO 6 configuration Web page)
- Firebox System Manager
- HostWatch
- Ping

To start any of these tools, click the link for the tool from the Tools section on the SOHO 6 management page.

Adding a Firebox SOHO 6 VPN Tunnel

The Firebox SOHO 6 management page shows all tunnels that include the device in the Tunnels section. You can also add a VPN tunnel in this section.

1 On the Firebox SOHO 6 management page, find the VPN Tunnels section.



This section shows all tunnels that include this device.

2 Click **Add** to add a new VPN tunnel.
The Add VPN Wizard starts. Configure the VPN to match your VPN requirements.

Creating and Applying Edge Configuration Templates

When you use Firebox® X Edge devices with the WatchGuard® Management Server, you can create Edge Configuration Templates on the Management Server. You can then apply those Edge Configuration Templates to Edge devices. With Edge Configuration Templates, you can easily configure standard firewall filters, change the blocked sites list, change your WebBlocker configuration, or change other policy settings for all or some of your managed Edge devices.

Note

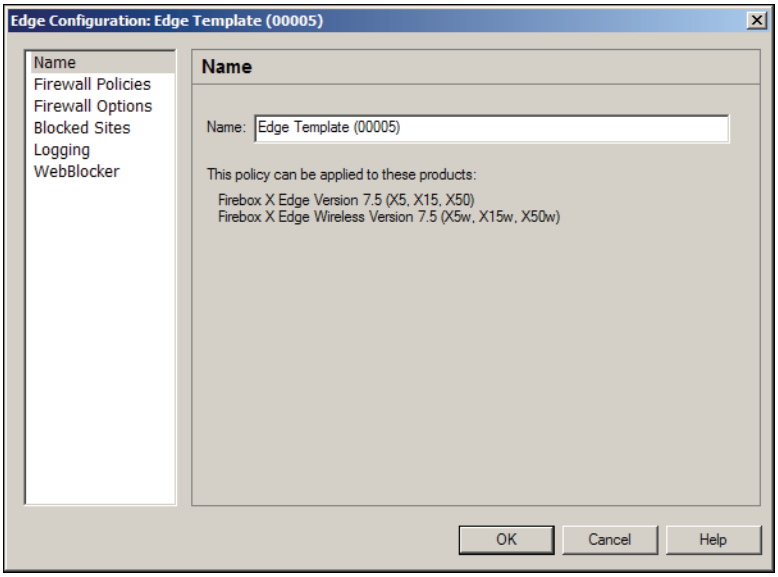
Edge Configuration Templates can be used with the Firebox X Edge only. Each Edge can have only one Edge Configuration Template. An Edge must have firmware version 7.5 or later to use Edge Configuration Templates.

You can make changes to an Edge Configuration Template or the list of devices to which the policy has been applied at any time. The Management Server automatically makes the changes.

1 Start WatchGuard System Manager and connect to the Management Server.

2 Click the **Device Management** tab.
You can expand the list of Edge Configuration Templates to see any Edge Configuration Templates that have been created. If you have not created any Edge Configuration Templates, this list is empty.

3 Right-click and select **Insert Edge Configuration Template**.



4 Type a name for the policy.

5 To configure the policy, click each category of settings in the left pane of the dialog box and type information in the fields that appear. The categories are:

- Firewall policies
- Firewall options
- Blocked sites
- Logging
- WebBlocker

For information on the fields that appear, see the *Firebox X Edge User Guide*.

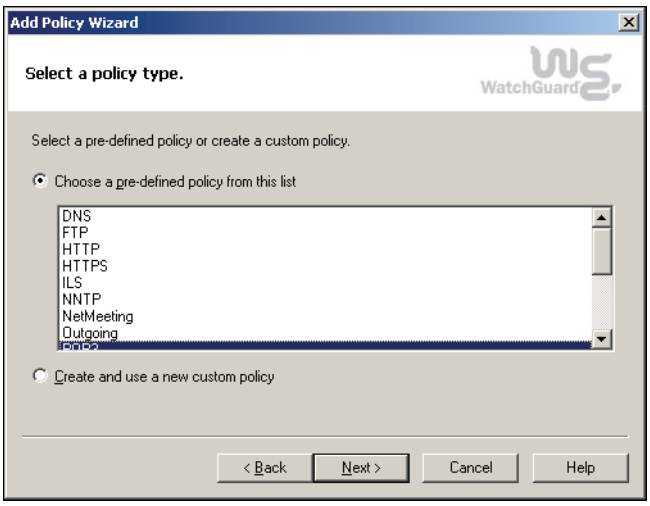
6 Click **OK** to close the Edge Configuration Template configuration.

The policy is saved to the Management Server, and an update is sent to all Firebox X Edge devices to which this policy is applied.

Adding a pre-defined policy with the Add Policy wizard

1 From the Device Management tab, right-click **Edge Configuration Templates** and select **Insert Edge Configuration Template**. Select **Firewall Policies** and click **Add**. The Add Policy wizard starts.

2 The Welcome page appears. Click **Next**.
The Select a policy type page appears.



3 To use a pre-defined policy, select **Choose a pre-defined policy from this list** and select the policy to use from the list.

4 Click **Next**.

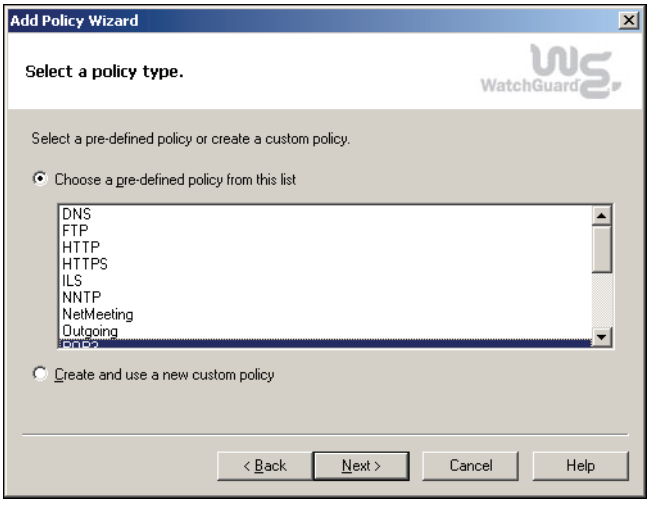
5 If you use a pre-defined policy, select the traffic direction.

6 Select to deny or allow traffic for this policy and direction.

Adding a custom policy with the Add Policy wizard

1 Start the Add Policy wizard. To do this, on the Firewall Policies page, click **Add** in the **Edge Configuration** dialog box.

2 The Welcome page appears. Click **Next**.

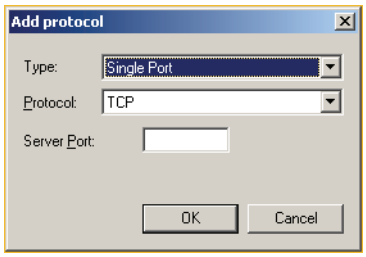


3 To create and use a custom policy, select **Create and use a new custom policy**.

4 Click **Next**.
The Specify Protocols page appears.

5 Type a name for the protocol.

6 To add a protocol, click **Add**.
The Add protocol dialog box appears.



7 Select to filter the TCP, UDP, or IP protocol.

8 Select one port or a range.

9 Type the port number or numbers, or the IP protocol number. Click **OK** to add the protocol.

10 Select the traffic direction. Select **Incoming**, **Outgoing**, or **Optional**.

11 Click **Add** to add another protocol. Click **Next** when all the protocols for this policy are added.

12 Select **Allow** or **Deny** for the filter action.
If the action is **Allow**, add the **From** and **To** destinations as required.

13 Click **Next**.

14 Click **Finish** to finish the wizard and return to the Edge Configuration dialog box.

Cloning an Edge Configuration Template

To clone, or copy, a template is useful when you have devices that use similar configurations, with slight variations. You can make one Edge Configuration Template, and then clone that policy for each variation, and make changes to those cloned templates.

1 Expand **Edge Configuration Templates** in the Device Management pane.

2 Right-click the Edge Configuration Template to be cloned, and select **Clone**.
A copy of the Edge Configuration Template appears in the list of Edge Configuration Templates.

3 Edit the cloned policy.

Applying an Edge Configuration Template to devices

You can apply the same Edge Configuration Template to one Firebox X Edge, or a group of Edge devices, at the same time. You cannot apply more than one Edge Configuration Template to one Edge.

Applying the policy using drag-and-drop

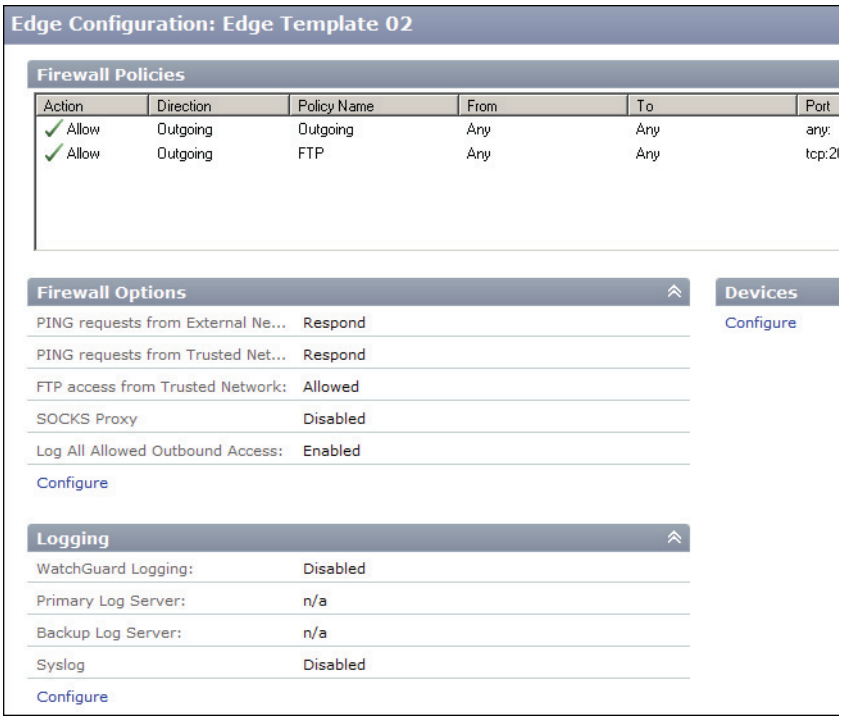
You can add an Edge Configuration Template to a Firebox X Edge device by drag-and-drop. Click the Edge device in the Devices list. Drag the Edge over the Edge Configuration Template in the Edge Configuration Templates list, and drop it on the policy. The policy is added to the Edge.

If you have a folder of devices, you can drag the folder over the Edge Configuration Template to apply the Edge Configuration Template to all Edge devices in the folder. All other devices are skipped.

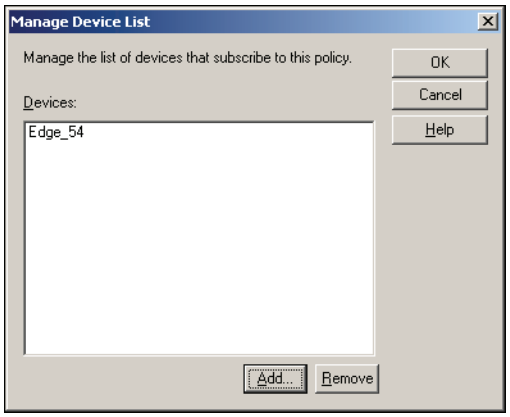
Applying the policy to devices in the device list

1 In the WatchGuard System Manager **Device Management** tab, expand the list of Edge Configuration Templates.

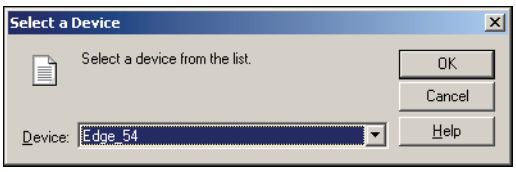
2 Select the policy to add to a device.
The policy configuration appears in the right frame of the window.



3 Click the **Configure** link below the **Devices** section.
The Manage Devices List appears.



4 Click **Add** to add a device to the list.
The Select Device dialog box appears.



5 Select a Firebox X Edge device from the drop-down list.

6 Click **OK**. Click **OK** again.
The managed devices you select are subscribed to the Edge Configuration Template.

Managing Firebox X Edge Network Settings

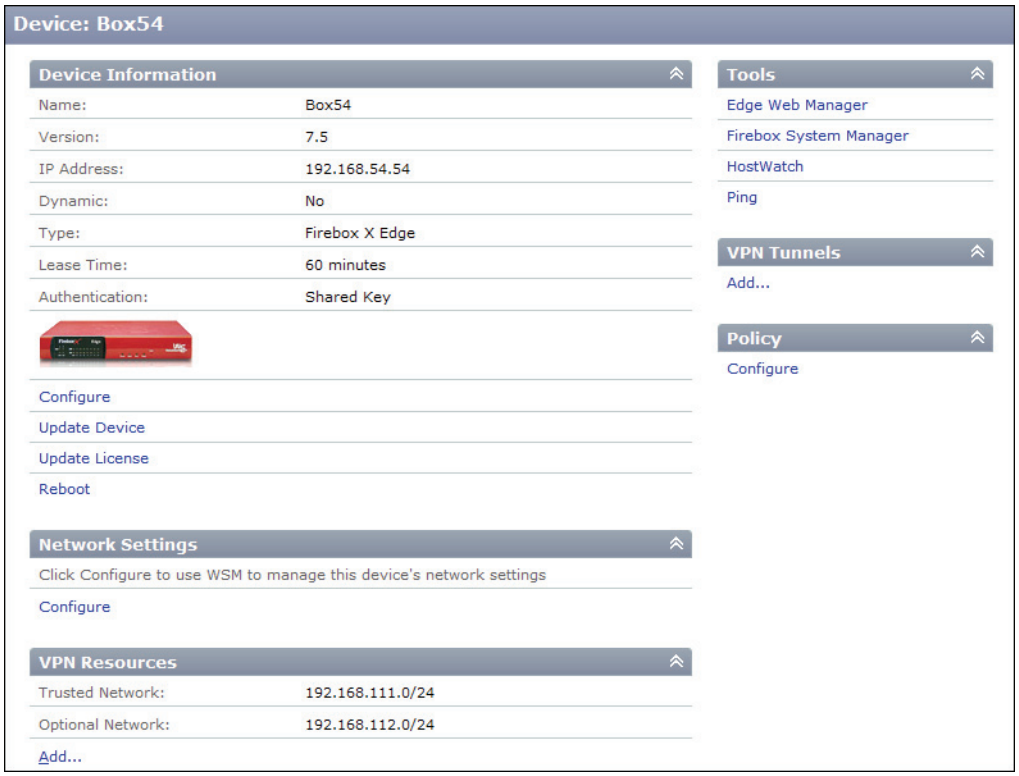
With a WatchGuard® Management Server, you can configure the network settings for a group of Firebox® X Edge devices using WatchGuard System Manager. You can use WatchGuard System Manager to configure the unique network settings for each Firebox X Edge. If the network settings for an Edge are already correct, you do not have to change them with WatchGuard System Manager, but you can if you want to.

Note

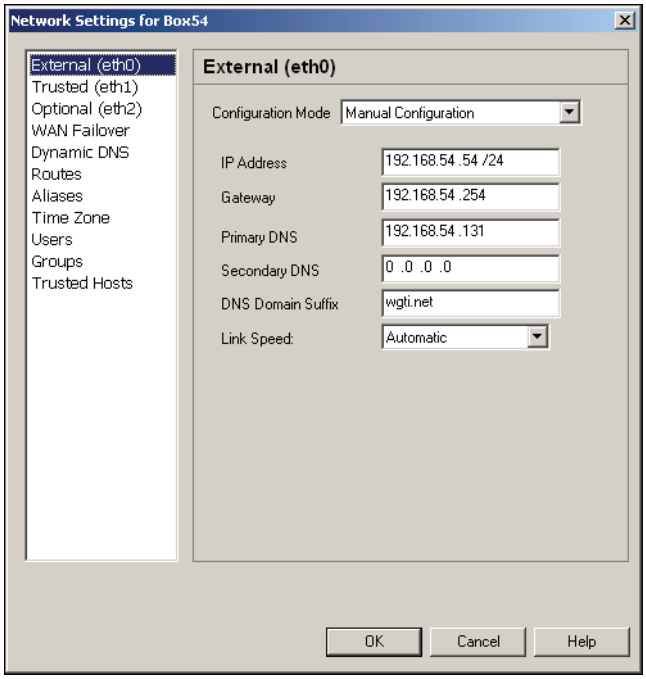
All Firebox X Edge network settings can be configured using the Edge web interface. For detailed information on these configuration options, see the *Firebox X Edge User Guide*.

1 Click the **Device Management** tab on WatchGuard System Manager.

2 Expand **Devices**, and click on a Firebox X Edge device.
The Edge configuration appears in the right pane.



3 Below Network Settings, click **Configure**. If you see a warning, click **OK**.
The Edge Network Settings dialog box appears.



4 To configure network settings, click each category of settings in the left pane of the dialog box and provide information in the fields that appear. The categories are:
   - External (eth0)
   - Trusted (eth1)
   - Optional (eth2)
   - WAN Failover
   - Dynamic DNS
   - Routes
   - Aliases (For more information about aliases, see the subsequent section, "Using Aliases.")
   - Time Zone
   - Users
   - Groups
   - Trusted Hosts

   For information on the fields that appear, see the *Firebox X Edge User Guide*.
5 Click **OK** to complete the configuration.

Using Aliases

Aliases are used with managed Firebox® X Edge devices to define a common destination for policy configuration on the Management Server. For example, with aliases, you can create an Edge Configuration Template for e-mail, and define that policy to operate with your e-mail server. Because the e-mail server can have a different IP address on each Firebox X Edge network, you create an alias on the Management Server called MailServer. When you create the Edge Configuration Template for the e-mail server, you use this alias as the destination. Then you define that alias as either the source or destination, depending on the direction of the policy. In this example you can configure an incoming SMTP Allow policy with MailServer as the destination.

To make the Edge Configuration Template operate correctly on Edge devices that use the policy, you configure the MailServer alias in the Network Settings for each Firebox X Edge device.

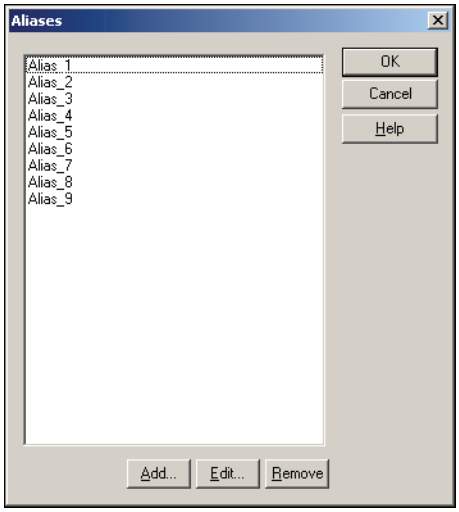
Alias configuration is done in two steps:

- Naming aliases on the Management Server
- Defining alias IP addresses on the Firebox X Edge

Naming aliases on the Management Server

1 In the **Device Management** tab in WatchGuard® System Manager, select the Management Server.
The Management Server settings page appears.

2 Click **Manage Aliases**.
The Aliases dialog box appears.



3 Select an alias and click **Edit** to edit the name.

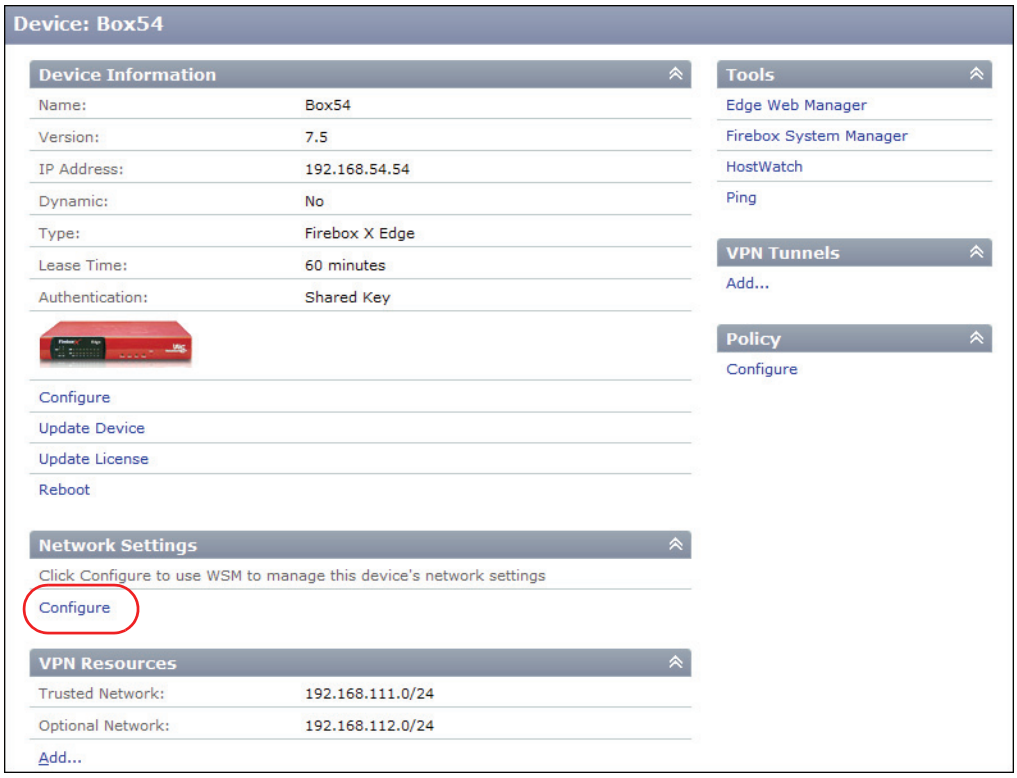
4 Type a name for the alias and click **OK**.

5 Repeat this procedure for all aliases that you must define.

6 Click **OK** when all aliases are configured.

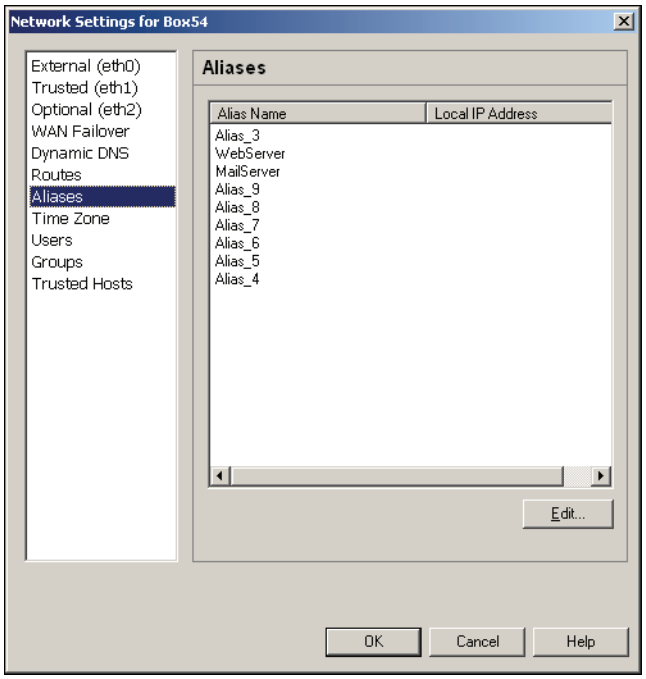
Defining aliases on a Firebox X Edge

1 In the **Device Management** tab in WatchGuard System Manager, select the Firebox X Edge.
The Management Server settings page appears.



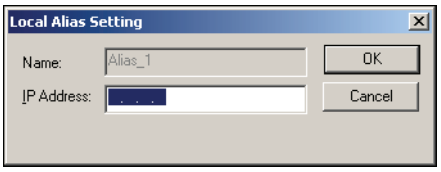
2 Click **Configure** under the **Network Settings** section.
The Network Settings dialog box appears.

3 Click **Aliases**.



The aliases appear. The aliases you named on the Management Server appear with those names in this dialog box.

4 Select an alias to define and click **Edit**.
The Local Alias Setting dialog box appears.



5 Type the IP address for the local alias on the network of this Firebox X Edge. Click **OK**.

6 Repeat the procedure for each alias to define.

7 Click **OK** when all aliases are defined.

CHAPTER 22

Configuring RUVPN with PPTP

Remote User Virtual Private Networking (RUVPN) uses Point-to-Point Tunneling Protocol (PPTP) to make a secure connection. It supports as many as 50 users at the same time for each Firebox®. RUVPN users can authenticate to the Firebox or to a RADIUS authentication server. You must configure the Firebox and the remote host computers of the remote user.

Configuration Checklist

Before you configure a Firebox® to use RUVPN, record this information:

- The IP addresses for the remote client to use for RUVPN sessions. **These IP addresses cannot be addresses that the network behind the Firebox uses.** The safest procedure to give addresses for RUVPN users is to install a "placeholder" secondary network with a range of IP addresses. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.0/24. Select the IP addresses in this subnet for your range of PPTP addresses. For more information, see "IP Addressing" on page 152.
- The IP addresses of the DNS and WINS servers that resolve host names to IP addresses.
- The user names and passphrases of users that are allowed to connect to the Firebox with RUVPN.

Encryption levels

For RUVPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The Firebox always tries to use 128-bit encryption first. It uses 40-bit encryption (if enabled) if the client cannot use the 128-bit encrypted connection.

For information on how to enable the drop from 128-bit to 40-bit, see "Preparing the Client Computers" on page 284.

If you do not live in the U.S. and you must have strong encryption allowed on your LiveSecurity Service account, send an e-mail to supportid@watchguard.com and include in it:

- Your LiveSecurity Service key number
- Date of purchase
- Name of your company

- Company mailing address
- Telephone number and name
- E-mail address

If you live in the U.S., you must download the strong encryption software from your archive page in the LiveSecurity™ Service web site. Go to www.watchguard.com, click **Support**, log in to your LiveSecurity Service account, and then click **Latest Software**. Download WatchGuard System Manager with strong encryption.

Then, uninstall WatchGuard System Manager, and install WatchGuard System Manager with strong encryption software from the downloaded file.

Note

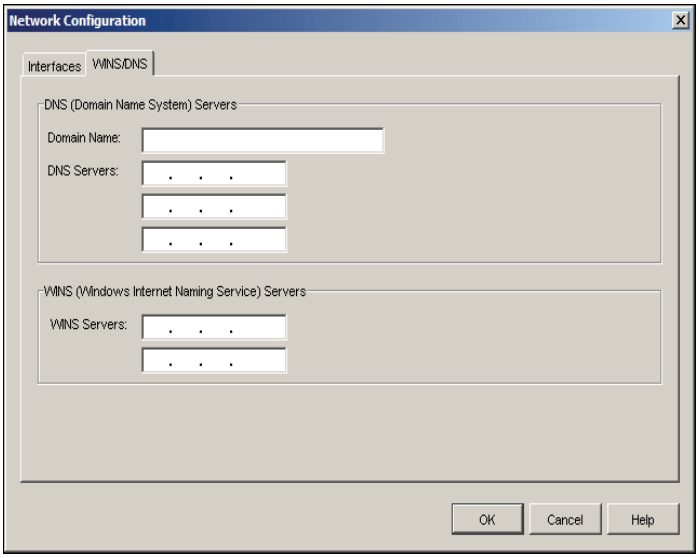
To keep your current Firebox configuration, do not use the Quick Setup Wizard when you install the new software. Open System Manager, connect to the Firebox, and save your configuration file. Configurations with a different encryption version are compatible.

Configuring WINS and DNS Servers

RUVPN clients use shared Windows Internet Naming Service (WINS) and Domain Name System (DNS) server addresses. DNS changes host names into IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the Firebox® must have access to these servers.

1 From Policy Manager, click **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.

2 In the IP address text boxes, type the addresses for the WINS and DNS servers. You can type three addresses for DNS servers, and two addresses for WINS servers. Type a domain name for the DNS server.



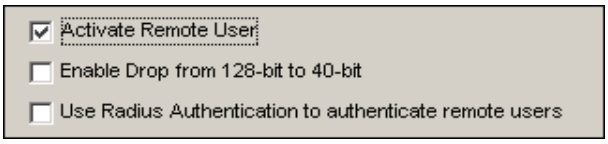
Enabling RUVPN with PPTP

To configure RUVPN with PPTP you must enable the feature. RUVPN with PPTP adds the WatchGuard® PPTP policy icon to Policy Manager. This sets default properties for PPTP connections and for the traffic that flows to and from them. We recommend that you do not change the default properties of the WatchGuard PPTP policy.

1 From Policy Manager, click **VPN > Remote Users**. Click the **PPTP** tab.

2 Select the **Activate Remote User** check box.

3 If necessary, select the **Enable Drop from 128-bit to 40-bit** check box.
Usually, only customers outside the United States use this check box.



Enabling extended authentication

RUVPN with extended authentication lets users authenticate to a RADIUS authentication server as an alternative to the Firebox®. For more information on extended authentication, see “Extended authentication” on page 151.

1 Select the **Use RADIUS Authentication to authenticate remote users** check box. Refer to the figure in the previous section.

2 Configure the RADIUS server in the **Authentication Servers** dialog box. Refer to “Implementing Authentication,” on page 111.

3 On the RADIUS server, create a PPTP-Users group and add names or groups of PPTP users.

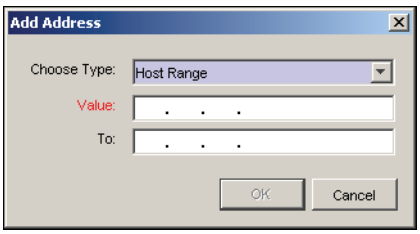
Adding IP Addresses for RUVPN Sessions

RUVPN with PPTP gives support to as many as 50 users at the same time. The Firebox® gives an open IP address to each incoming RUVPN user from a group of available addresses. This goes on until all the addresses are in use. After a user closes a session, the address is put back in the available group. The subsequent user who logs in gets this address.

For more information about how to get IP addresses for RUVPN clients, see “IP Addressing” on page 152. You must configure two or more IP addresses for PPTP to operate correctly.

From the **PPTP** tab on the **Remote Users Configuration** dialog box:

1 Click **Add**.
The Add Address dialog box appears.



2 From the **Choose Type** drop-down list, select **Host IP** (for a single IP address) or **Host Range** (for a range of IP addresses).

You can configure 50 addresses. If you select Host IP, you must add at least two IP addresses. If you select Host Range and add a range of IP addresses that is larger than 50 addresses, RUVPN with PPTP uses the first 50 addresses in the range.

3 In the **Value** text box, type the host IP address. If you selected **Host Range**, type the first and last IP address in the range. Click **OK**.

Type IP addresses that are not in use that the Firebox can give to clients during RUVPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.

4 Do the procedure again to configure all the addresses for use with RUVPN with PPTP.

Adding New Users to the PPTP_Users Authentication Group

To create a PPTP VPN tunnel with the Firebox®, a remote user types their user name and password to authenticate. WatchGuard® System Manager software uses this information to authenticate the user to the Firebox.

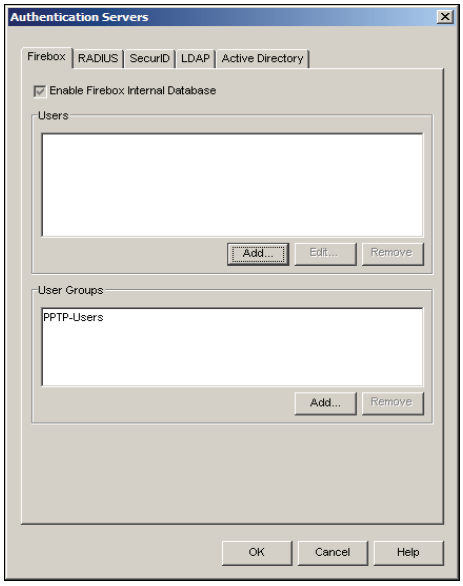
When you enable PPTP in your Firebox configuration, a default user group is created automatically. This user group is called pptp_users. You see this group name when you create a new user or add user names to policies.

For more information on Firebox groups, see “Implementing Authentication,” on page 111.

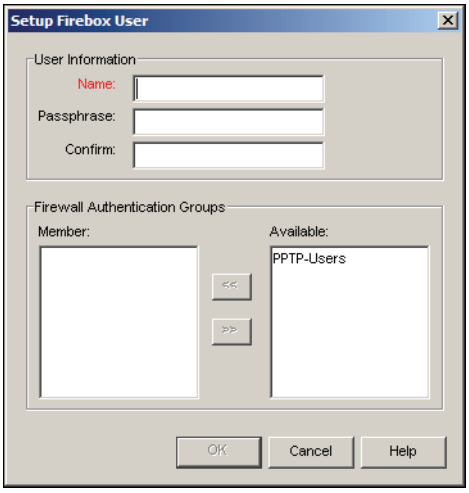
1 From Policy Manager, click **Setup > Authentication Servers**.

The Authentication Servers dialog box appears.

2 Click the **Firebox** tab.



3 To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox User dialog box appears.



4 Type a user name and passphrase for the new user. Type the passphrase again to confirm it.
The new user is put on the Users list. The Authentication Servers dialog box stays open so you can add more users.

5 To close the **Authentication Servers** dialog box, click **OK**.
You can use the users and groups to configure policies. See the subsequent section.

Configuring Policies to Allow Incoming RUVPN Traffic

RUVPN users have no access privileges through a Firebox®. You must add user names or the full PPTP-Users group to policies to give remote users access to specified network resources.

WatchGuard® recommends two procedures to configure the policies for RUVPN traffic: individual policies or the Any policy. It is best to configure individual policies to control RUVPN traffic. The Any policy opens a hole through the Firebox for authenticated RUVPN users. This lets all the traffic flow between hosts and does not apply firewall rules. This is a security risk.

By individual policy

In Policy Manager, double-click a policy to enable for your VPN users. It is a good idea to create a new policy specially for PPTP traffic and keep it separate from your other firewall policies. To set the properties:

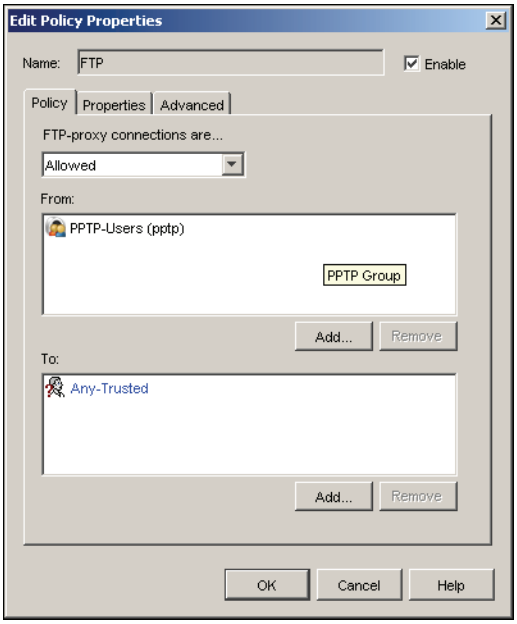
For an incoming policy:

- Allowed
- From: PPTP users or groups
- To: trusted, optional, network or host IP address, or alias

For an outgoing policy:

- Allowed
- From: trusted, optional, network or host IP address, or alias

- To: PPTP users or groups



Using the Any policies

Add Any policies with these properties:

Incoming policy:

- Allowed
- From: PPTP users or groups
- To: trusted, optional, network or host IP address, or alias

Outgoing policy:

- Allowed
- From: trusted, optional, network or host IP address, or alias
- To: PPTP users or groups

Make sure that you save your configuration file to the Firebox after you make these changes.

Note

To use WebBlocker to control the access of remote users, add PPTP users or groups to a proxy policy that controls WebBlocker, such as HTTP-proxy. Use this type of policy with any packet filter or proxy policy as an alternative to the Any policy.

Preparing the Client Computers

You must first prepare each computer that you use as an RUVPN with PPTP remote host with Internet access. Then, do these procedures using the instructions in the subsequent sections:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections

- Install a VPN adapter (not necessary for all operating systems).

Installing MSDUN and service packs

It can be necessary to install these options for the correct configuration of RUVPN:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- Other extensions
- Service packs

For RUVPN with PPTP, it is necessary to install these upgrades:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2

*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98, with strong encryption, Windows 2000 will automatically set strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center Web site at:

http://www.microsoft.com/downloads/search.asp

Creating and Connecting a PPTP RUVPN on Windows XP

To prepare a Windows XP remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1 Click **Start > Control Panel > Network Connections**.
The Network Connection wizard appears.

2 Click **Create a new connection** from the menu on the left. The New Connection wizard starts. Click **Next**.

3 Click **Connect to the network at my workplace**. Click **Next**.

4 Click **Virtual Private Network Connection**. Click **Next**.

5 Give the new connection a name, such as "Connect with RUVPN." Click **Next**.

6 Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.
The wizard includes this screen if you use Windows XP SP2. Not all Windows XP users see this screen.

7 Type the host name or IP address of the Firebox® external interface. Click **Next**.

8 Select who can use this connection profile. Click **Next**.

9 Select **Add a shortcut to this connection to my desktop**. Click **Finish**.

10 To connect with your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.

11 Double-click the shortcut to the new connection on your desktop.
Or, select Control Panel > Network Connections and look in the Virtual Private Network list for the connection you created.

12 Type the user name and passphrase for the connection.
This information was given when you added the user to pptp_users. See "Adding New Users to the PPTP_Users Authentication Group" on page 282.
13 Click **Connect**.

Creating and Connecting a PPTP RUVPN on Windows 2000

To prepare a Windows 2000 remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1 Click **Start > Settings > Network Connections > Create a New Connection**.
The New Connection wizard appears.
2 Click **Next**.
3 Select **Connect to the network at my workplace**. Click **Next**.
4 Click **Virtual Private Network connection**.
5 Give the new connection a name, such as "Connect with RUVPN." Click **Next**.
6 Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.
7 Type the host name or IP address of the Firebox® external interface. Click **Next**.
8 Select **Add a shortcut to this connection to my desktop**. Click **Finish**.
9 To connect with your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.
10 Double-click the shortcut to the new connection on your desktop.
Or, select Control Panel > Network Connections and look in the Virtual Private Network list for the connection you created.
11 Type the user name and passphrase for the connection.
This information was given when you added the user to pptp_users. See "Adding New Users to the PPTP_Users Authentication Group" on page 282.
12 Click **Connect**.

Running RUVPN and accessing the Internet

You can enable remote users to get access to the Internet through a RUVPN tunnel. But this option has an effect on security. See "Tunneling Methods" on page 155.

1 When you set up your connection on the client computer, use the **Advanced TCP/IP Settings** dialog box to select the **Use default gateway on remote network** check box.
To open the Advanced TCP/IP Settings dialog box on Windows XP or Windows 2000, right-click the VPN connection in **Control Panel > Network Connections**. Select **Properties** and click the **Network** tab. Find **Internet Protocol** in the list box and click **Properties**. On the **General** tab, click **Advanced**.
2 Make sure that the IP addresses you have added to the PPTP address pool are included in your dynamic NAT configuration. To make sure, from Policy Manager select **Network > NAT**.
3 Edit your policy configuration to allow connections from PPTP-Users through the external interface. If you use WebBlocker to control remote user web access, add PPTP-Users to the policy that controls WebBlocker (such as HTTP-proxy).

Making outbound PPTP connections from behind a Firebox

If necessary, you can make a PPTP connection to a Firebox from behind a different Firebox. For example, a remote user goes to a customer office that has a Firebox. The user can make PPTP connections to their network with PPTP. For the local Firebox to correctly allow the outgoing PPTP connection, add the PPTP policy and allow PPTP to Any-External. For information on enabling policies, see the "Configuring Policies" chapter of this guide.

CHAPTER 23

Controlling Web Site Access with WebBlocker

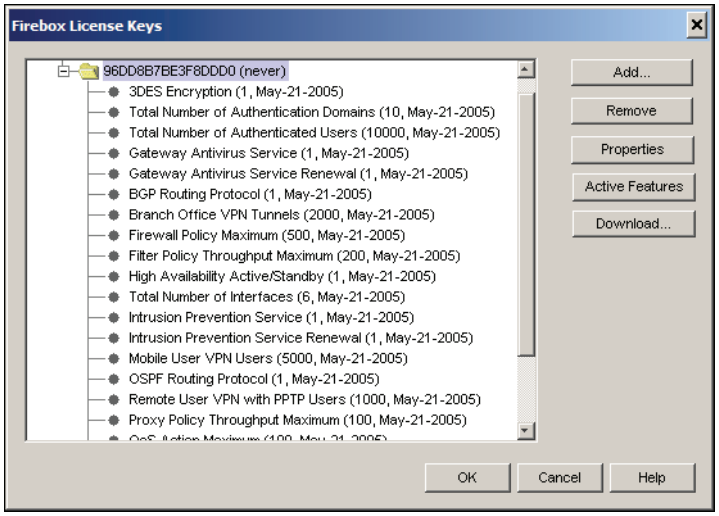
The WebBlocker feature of WatchGuard® Fireware® uses the HTTP proxy to control web traffic. You can select the exact hours in the day that users can browse the Internet. You can also select categories of web sites that users cannot go to.

Installing the Software Licenses

To install WebBlocker, you must have a WebBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

To install this feature key:

1 From Policy Manager, select **Setup > Licensed Features**.
The Firebox License Keys dialog box appears.


Firebox License Keys
96DD8B7BE3F8DDD0 (never)
3DES Encryption (1, May-21-2005)
Total Number of Authentication Domains (10, May-21-2005)
Total Number of Authenticated Users (10000, May-21-2005)
Gateway Antivirus Service (1, May-21-2005)
Gateway Antivirus Service Renewal (1, May-21-2005)
BGP Routing Protocol (1, May-21-2005)
Branch Office VPN Tunnels (2000, May-21-2005)
Firewall Policy Maximum (500, May-21-2005)
Filter Policy Throughput Maximum (200, May-21-2005)
High Availability Active/Standby (1, May-21-2005)
Total Number of Interfaces (6, May-21-2005)
Intrusion Prevention Service (1, May-21-2005)
Intrusion Prevention Service Renewal (1, May-21-2005)
Mobile User VPN Users (5000, May-21-2005)
OSPF Routing Protocol (1, May-21-2005)
Remote User VPN with PPTP Users (1000, May-21-2005)
Proxy Policy Throughput Maximum (100, May-21-2005)
Add...
Remove
Properties
Active Features
Download...
OK
Cancel
Help

2 Click **Remove** to remove the current feature key.
You must remove the entire feature key before you install the new one that includes WebBlocker.

3 Click **Add**.

4 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Firebox License Keys dialog box.

Getting Started with WebBlocker

You can install the WebBlocker Server on your WatchGuard® management station when you first do the setup for WatchGuard System Manager. You can also install the WebBlocker Server software on a different computer. To do this, use the same method as you used to install the WatchGuard System Manager software, but select only the WebBlocker Server component.

Operating systems that are supported for the WebBlocker Server are Windows 2000 and Windows 2003.

Note

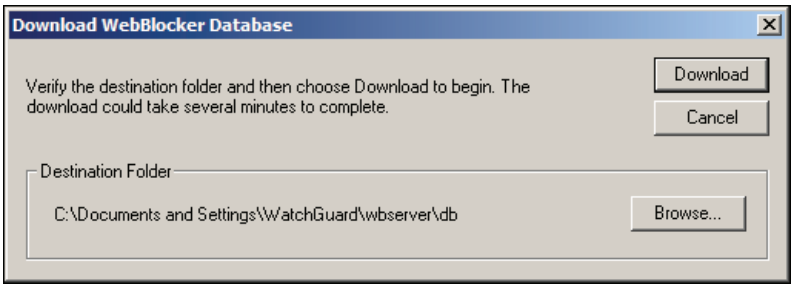
If you install one of the WSM servers on a computer with a personal firewall other than the Microsoft Windows firewall, you must open the ports for the servers to connect through the firewall. To allow connections to the WebBlocker Server, open UDP port 5003. It is not necessary to change your configuration if you use the Microsoft Windows firewall. See the "Getting Started" chapter for more information.

Before you configure WebBlocker, you must download the WebBlocker database.

1 Right-click the WebBlocker Server icon in the toolbar at the bottom of the screen.

2 Select **Get Full Database**.
The Download WebBlocker Database dialog box appears.

3 Select **Download** to download the new database.


Download WebBlocker Database
Verify the destination folder and then choose Download to begin. The download could take several minutes to complete.
Download
Cancel
Destination Folder
C:\Documents and Settings\WatchGuard\wbserver\db
Browse...

Note

The WebBlocker database has more than 95 MB of data. Your connection speed sets the download speed, and the download can be more than 30 minutes. Make sure the hard disk drive has a minimum of 200 MB of free space.

You can use the WebBlocker utility at any time to:

- Download a new version of the database
- See the database status
- Start or stop the server

To get an incremental update of the WebBlocker database, you must first stop the WebBlocker Server service. To stop the service, right click the WebBlocker Server icon on the WatchGuard toolbar and select **Stop Service**.

Automating WebBlocker database downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. You can use Windows Task Scheduler to schedule the "updatedb.bat" process, which is created automatically for you in your WSM8/bin directory.

1 Open **Scheduled Tasks**. To open the Task Scheduler using Windows XP, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.

2 Click **Add Scheduled Task**.

3 The Scheduled Tasks wizard starts. Click **Next**.

4 The screen shows a list of programs. Click **Browse**.

5 Go to C:\Program Files\WatchGuard\wsm8\bin. Select **updatedb.bat**.

6 Select the time interval at which to do this task. We recommend that you update your database each day. You can update less frequently if you have low bandwidth. Click **Next**.

7 Type the time and frequency to start the procedure. Because you must stop the WebBlocker Server to do the update, we recommend that you schedule updates outside of your usual hours of operation.

8 Select a start date. Click **Next**.

9 Type the user name and the password to use this procedure. Make sure that this user has access to the necessary files. Click **Next**.

10 Click **Finish**.

Activating WebBlocker

Before you use WebBlocker in an HTTP proxy policy, you must use the Activate WebBlocker wizard to activate the feature and create a basic configuration. To do this:

1 From WatchGuard® System Manager, select the Firebox® to use WebBlocker.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manger toolbar.

3 From Policy Manager, select **Tasks** > **WebBlocker** > **Activate**.
The Activate WebBlocker Wizard starts.

4 Click **Next**.

5 Click through the wizard and add the information it asks for. The wizard has these screens:

Select policies for WebBlocker

This screen does not appear if you have not yet defined any HTTP proxy policies. In this case, the wizard will create an HTTP proxy policy for you.

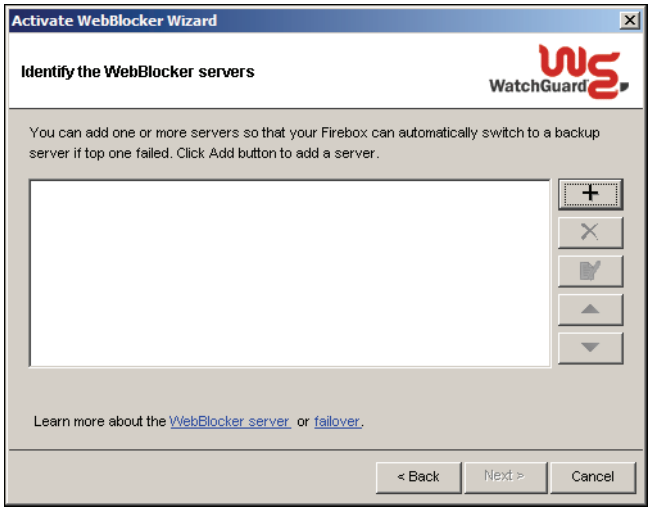
If HTTP proxy policies are already created on your Firebox, this screen shows them in a list. From the list, select the proxy policies you want to enable WebBlocker for. If no policy is selected, a new HTTP proxy policy is created with a WebBlocker action.

Identify the WebBlocker Servers

You must configure a minimum of one WebBlocker Server. To add a WebBlocker Server, click the plus sign (+). Next to **Server IP**, type the IP address of the WebBlocker Server. If necessary, change the port number.

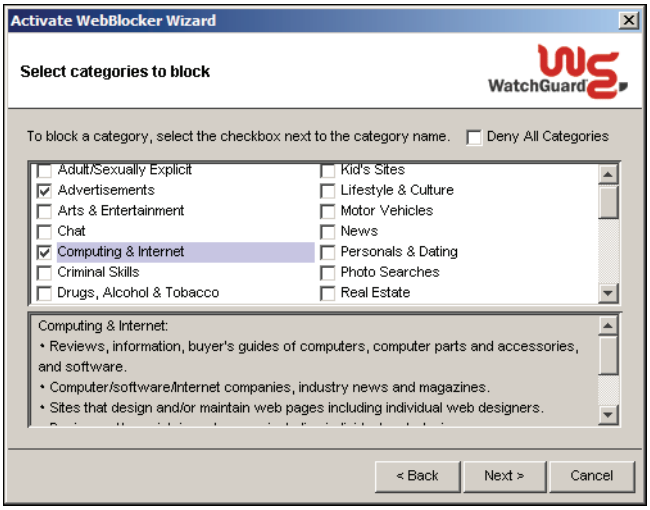
You can add more than one WebBlocker Server so the Firebox can fail over to a backup server if it cannot connect to the primary server. The first server in the list is the primary server.

To add a WebBlocker Server after you complete the wizard, go to **Setup** > **Actions** > **WebBlocker**. Add servers on the **Servers** tab.


Activate WebBlocker Wizard
Identify the WebBlocker servers
WatchGuard
You can add one or more servers so that your Firebox can automatically switch to a backup server if top one failed. Click Add button to add a server.
Learn more about the WebBlocker server or failover.
< Back
Next >
Cancel

Select categories to block

Select the check box adjacent to the categories of web sites you want to block. To read a description of the category, select the check box adjacent to it. The description appears in the box at the bottom of the screen. If you want to block access to web sites that match any category, select **Deny All Categories**.



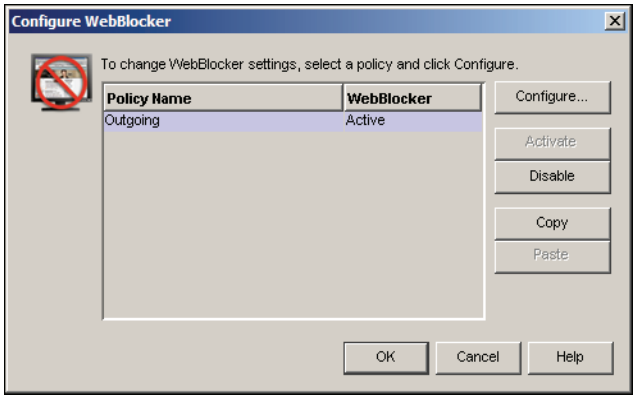
Note

To stop users from going to anonymizer web sites to try to avoid WebBlocker, block the Remote Proxies category in WebBlocker.

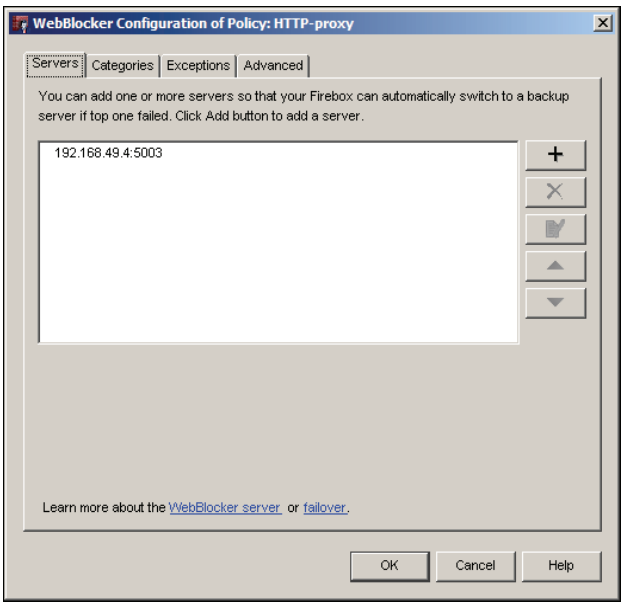
Configuring WebBlocker

After you use the Activate WebBlocker Wizard to activate WebBlocker and create a basic configuration, you can configure more WebBlocker settings.

1 From Policy Manager, select **Tasks** > **WebBlocker** > **Configure**.
The Configure WebBlocker dialog box appears and shows the HTTP policies that were already created.



2 Select the policy you want to configure and click **Configure**.
The WebBlocker Configuration dialog box for that policy appears.


WebBlocker Configuration of Policy: HTTP-proxy
Servers
Categories
Exceptions
Advanced
You can add one or more servers so that your Firebox can automatically switch to a backup server if top one failed. Click Add button to add a server.
192.168.49.4:5003
Learn more about the WebBlocker server or failover.
OK
Cancel
Help

The **WebBlocker Configuration** dialog box includes tabs to configure servers, categories, exceptions, and advanced settings.

Adding new servers

You can add more than one WebBlocker Server so the Firebox® can fail over to a backup server if it cannot connect to the primary server. The first server in the list is the primary server. You cannot add more than five WebBlocker Servers to a configuration.

1 To add a server, click the plus sign (+).
The Add WebBlocker Server dialog box appears.
2 Next to **Server IP**, type the IP address of the WebBlocker Server. Type the port number.

Selecting categories to block

When you used the Activate WebBlocker wizard, you selected categories of web sites you want to block. You can use this dialog box to make changes to your original configuration. Select the check box adjacent to the categories of web sites you want to block. To read a description of the category, click on it. The description appears in the box at the bottom of the screen. If you want to block access to web sites that match any category, select **Deny All Categories**.

Note

To stop users from going to anonymizer web sites to try to avoid WebBlocker, select to block the Remote Proxies category in WebBlocker.

Defining WebBlocker exceptions

You can override a WebBlocker action with an exception. You can add a web site that is allowed or denied as an exception to the WebBlocker categories. The web sites you add apply only to HTTP traffic. They are not added to the Blocked Sites list.

The exceptions are based on URL patterns, not IP addresses. You can have the Firebox block an URL with an exact match. Usually, it is more convenient to have the Firebox look for URL patterns. The URL patterns do not include the leading "http://". To match a URL path on all web sites, the pattern must have a leading "/*".

The host in the URL can be the host name specified in the HTTP request, or the IP address of the server.

Network addresses are not supported at this time, though you can use subnets in a pattern (for example, 10.0.0.*).

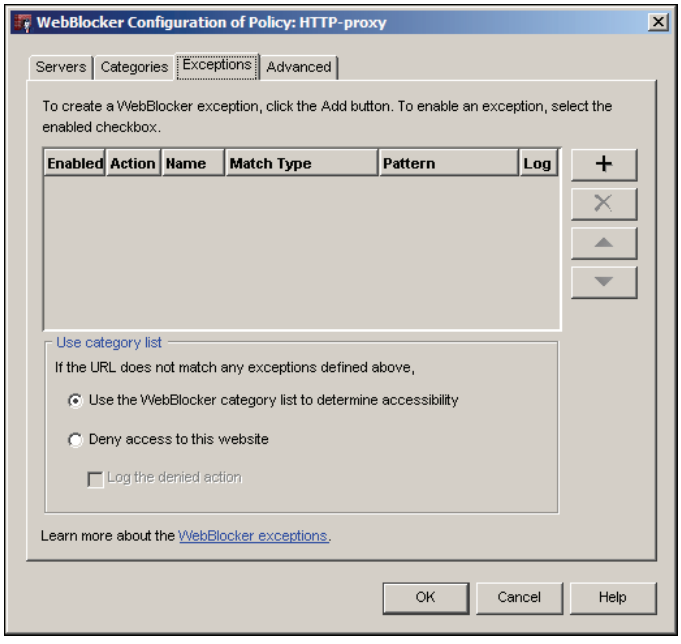
For servers on port 80, do not include the port. For servers on ports other than 80, add " :port", for example: 10.0.0.1:8080. You can also use a wildcard for the port—for example,10.0.0.1:*—but this does not apply to port 80.

You can create WebBlocker exceptions with the use of any part of a URL. You can set a port number, path name, or string that must be blocked for a special web site. For example, if it is necessary to block only www.sharedspace.com/~dave because it has inappropriate photographs, you type "www.sharedspace.com/~dave/*". This gives the users the ability to browse to www.sharedspace.com/~julia, which could contain content you want your users to see.

To block URLs that contain the word "sex" in the path, you can type "*/*sex*". To block URLs that contain "sex" in the path or the host name, type "*sex*".

You can block ports in an URL. For example, look at the URL http://www.hackerz.com/warez/index.html:8080. This URL has the browser use the HTTP protocol on TCP port 8080 instead of the default method that uses TCP 80. You can block the port by matching *8080.

1 To create exceptions to the WebBlocker categories, click the **Exceptions** tab.



2 Click the "+" sign to add a new exception rule.

3 Click the **Action** column to get access to the **Action** drop-down list. Select to have WebBlocker allow or deny the exception.

4 Type a name for the exception in the **Name** text box.

5 Click the **Match Type** column to get access to the **Match Type** drop-down list:

Pattern match: Be sure to drop the leading "http://" and include "/* at the end.

Exact match: Select this to match character by character. If you enter an exception to allow www.yahoo.com as an exact match only, and a user types "www.yahoo.com/news", the request is denied.

Regular expression: Supports wild cards used in shell script

6 Type the pattern you want to identify as an exception in the **Pattern** text box.

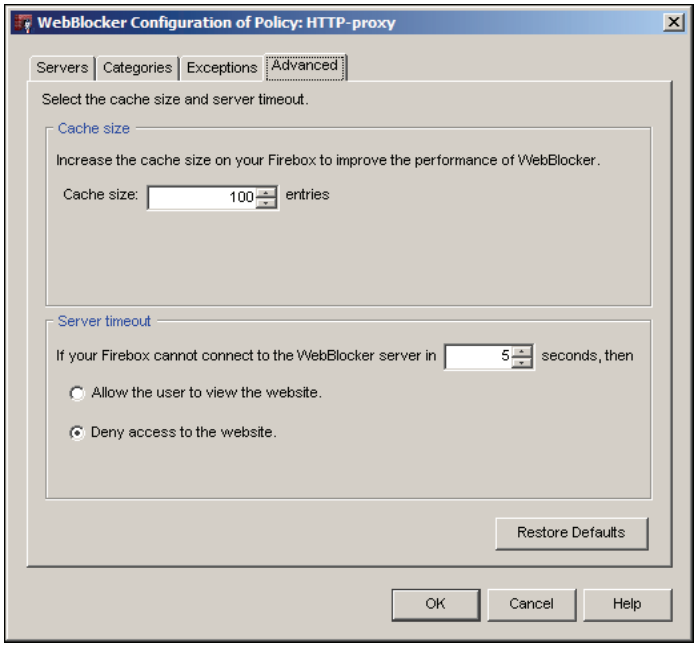
7 Click the **Log** check box if you want a log message when an action is taken on a WebBlocker exception.

8 To enable the exception, click the **Enabled** check box.

9 In the **Use category list** section, you can configure the action to occur if the URL does not match the exceptions you configure. If you want to use the list on the **Categories** tab to determine accessibility, click the top radio button. If you want to deny access, click the bottom radio button. If you deny access, you can select the check box below the radio button to send a log message for that action.

Defining advanced WebBlocker options

1 To configure advanced WebBlocker options, click the **Advanced** tab.



2 You can adjust the **Cache size** setting to improve WebBlocker performance. Use the arrows to change the number of entries in the cache or type in a number.

3 You can set a time-out value and an action to occur when the server times out. If you want to allow the web site if the server times out, select **Allow the user to view the website**. If you want to deny the web site, select **Deny access to the website**.

Scheduling a WebBlocker Action

You can set an operating schedule for the policy. You can use the predefined settings in the drop-down list or create custom schedules. You use these time periods to set rules for when to block different web sites. For example, you can block sports web sites during usual business hours of operation, but allow users to browse at lunch time, evenings, and weekends.

To set a schedule for a policy

1 Open the policy to edit it, and click the **Advanced** tab.

2 Select a schedule from the drop-down list, or click the New/Clone icon to make a new schedule. For more information, see "Creating Schedules" on page 50.

3 Configure an HTTP policy that uses the schedule.

You can also configure two HTTP policies, but create a schedule for only one of them. Each policy uses one of the HTTP proxy actions. Each of these HTTP proxy actions points to one of at least two WebBlocker actions.

CHAPTER 24

Configuring spamBlocker

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources.

The WatchGuard® spamBlocker™ option uses industry-leading pattern detection technology from Commtouch® to block spam at your Internet gateway and keep it from getting to your e-mail server. spamBlocker looks for patterns in spam attacks, instead of the contents of individual e-mail messages. Because it looks for patterns, it can detect spam in any language, format, or encoding method.

About spamBlocker

Before you install spamBlocker™, you must have:

- A spamBlocker license key certificate
- An SMTP e-mail server behind the Firebox®
- A SMTP Proxy policy
- DNS configured on the Firebox. From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab and type the IP addresses of the DNS servers your Firebox uses to resolve host names.

spamBlocker actions

The Firebox uses spamBlocker actions to apply decisions about the delivery of an e-mail message that is spam. It can:

- **Deny** — Stop the spam e-mail message from being delivered to the mail server with no reply to the sender.
- **Tag** —Identify the e-mail message as spam or not spam and allow spam e-mail messages to go to the mail server. See the subsequent section for more information on spamBlocker tags.
- **Allow** — Let spam e-mail messages go through the Firebox without a tag.

spamBlocker tags

The Firebox can add spamBlocker tags to the subject line of the e-mail message. You can also configure spamBlocker to customize the tag that it adds. This example shows the subject line of an e-mail message that was found to be spam. The tag added is the default tag: ***SPAM***.

```
Subject: ***SPAM*** Free auto insurance quote
```

This example shows a custom tag: [SPAM]

```
Subject: [SPAM] You've been approved!
```

spamBlocker categories

spamBlocker looks at e-mail messages to find matches to the patterns in the spamBlocker database. It puts spam e-mail into three categories: Spam, Bulk, and Suspect. spamBlocker assigns e-mail messages to these categories based on the number of patterns found in the e-mail message.

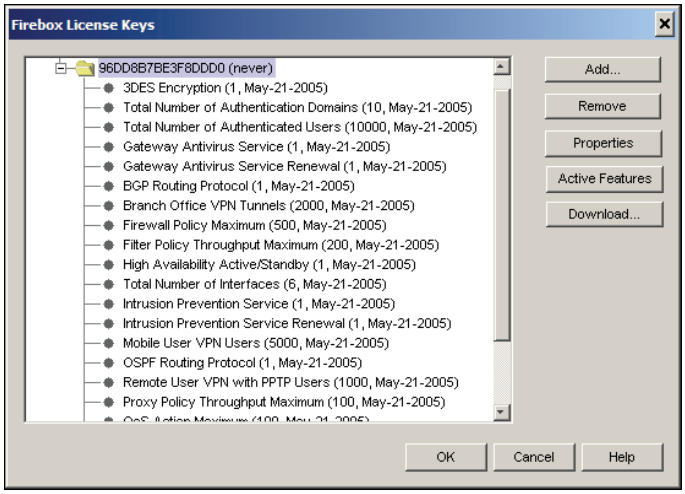
- The *Spam* category includes e-mail messages that come from known spammers. We recommend you use the Deny action for this type of e-mail.
- The *Bulk* category includes e-mail messages that do not come from known spammers, but do match some known spam structure patterns. We recommend that you use the Tag action for this type of e-mail.
- The *Suspect* category includes e-mail messages that look like e-mail messages that could be associated with a new spam attack. Frequently, these messages are legitimate e-mail messages. We recommend that you use the Tag action for this type of e-mail.

Installing the Software License

To install spamBlocker™, you must have a spamBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

To install this feature key:

1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.


Firebox License Keys
96DD8B7BE3F8DDD0 (never)
3DES Encryption (1, May-21-2005)
Total Number of Authentication Domains (10, May-21-2005)
Total Number of Authenticated Users (10000, May-21-2005)
Gateway Antivirus Service (1, May-21-2005)
Gateway Antivirus Service Renewal (1, May-21-2005)
BGP Routing Protocol (1, May-21-2005)
Branch Office VPN Tunnels (2000, May-21-2005)
Firewall Policy Maximum (500, May-21-2005)
Filter Policy Throughput Maximum (200, May-21-2005)
High Availability Active/Standby (1, May-21-2005)
Total Number of Interfaces (6, May-21-2005)
Intrusion Prevention Service (1, May-21-2005)
Intrusion Prevention Service Renewal (1, May-21-2005)
Mobile User VPN Users (5000, May-21-2005)
OSPF Routing Protocol (1, May-21-2005)
Remote User VPN with PPTP Users (1000, May-21-2005)
Proxy Policy Throughput Maximum (100, May-21-2005)
Add...
Remove
Properties
Active Features
Download...
OK
Cancel
Help

2 Click **Remove** to remove the current feature key.
You must remove the entire feature key before you install the new one that includes spamBlocker.

3 Click **Add**.

4 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

Activating spamBlocker

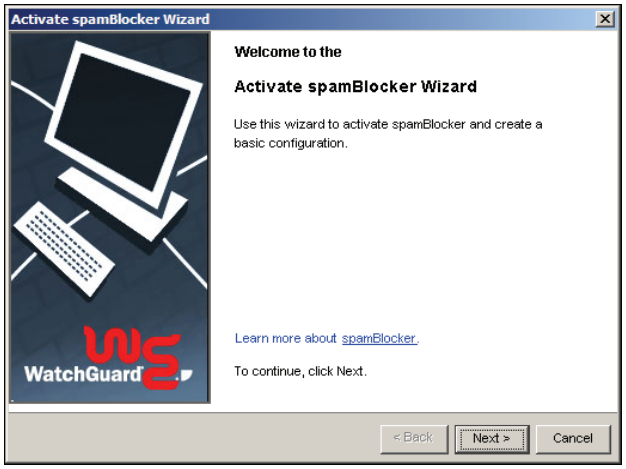
To activate spamBlocker™, you use a wizard that starts the feature and creates a basic configuration.

1 From WatchGuard System Manager, select the Firebox that will use spamBlocker.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manager toolbar.

3 From Policy Manager, select **Tasks** > **spamBlocker** > **Activate**.
The Activate spamBlocker wizard starts.



4 Click through the wizard and add the information it asks for. The wizard has these screens:

Apply spamBlocker settings to your policies

This screen appears if you already have one or more SMTP policies defined on your Firebox but do not have spamBlocker enabled. From the list, select the proxy policies for which you want to enable spamBlocker. Any policies that have spamBlocker already enabled are grayed out. If you do not have any SMTP policies defined at this time, this screen does not appear.

Create proxy policies

This screen appears if your Firebox does not yet have a policy created for SMTP. The wizard will create an SMTP proxy policy for you. You must have at least one external interface with a static IP address.

To create an SMTP policy, enter the e-mail server IP address. The policy created by this wizard contains "Any-External" for the **From** field and a static NAT entry for the **To** field. The static NAT entry uses the first static external IP address configured on the Firebox. It enables static NAT for the e-mail server IP address you enter in the wizard. If this default static NAT SMTP policy is not the best choice for your organization, you can use Policy Manager to create an SMTP policy before you use the wizard.

Select the spamBlocker actions

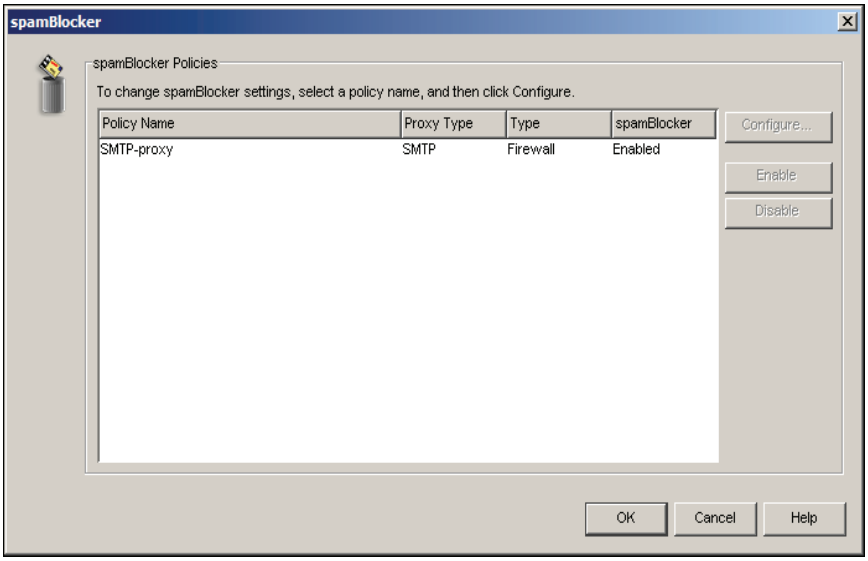
Use this screen to select the spamBlocker actions for e-mail in the Spam, Bulk, and Suspect categories.

If you want to record log messages for a spamBlocker response, select the **Log** check box. If you do not want to record log messages, clear the **Log** check box.

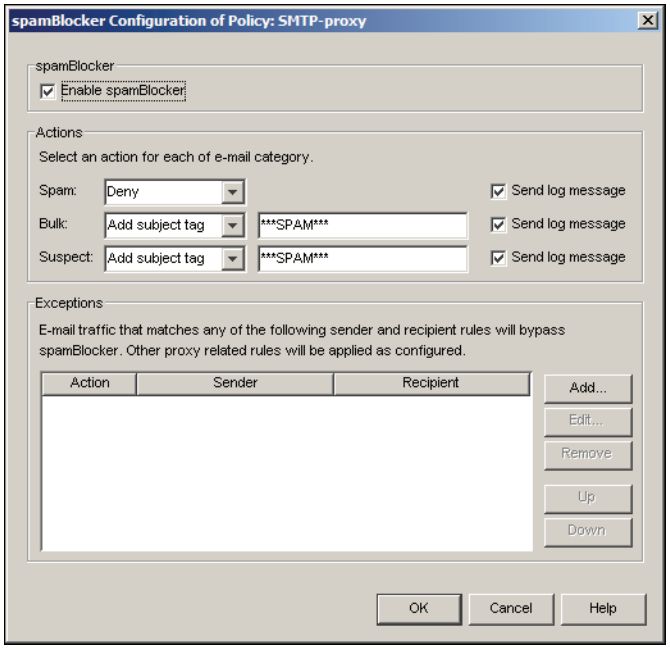
Configuring spamBlocker

After you use the Activate spamBlocker wizard to activate spamBlocker and create a basic configuration, you can set other configuration parameters.

1 From Policy Manager, select **Tasks** > **spamBlocker** > **Configure**.
The spamBlocker dialog box appears with SMTP policies in a list. It shows if spamBlocker is enabled for each policy.



2 Select the policy you want to configure and click **Configure**.
The spamBlocker Configuration page for that policy appears.



3 When you used the Activate spamBlocker wizard, you set the actions spamBlocker applies for e-mail in the Spam, Bulk, and Suspect categories. You can change the actions in this dialog box.

4 If you want to record log messages for a spamBlocker response, select the **Log** check box for the action. If you do not want to record log messages, clear the **Log** check box.

5 Make sure DNS is enabled on the Firebox that applies spamBlocker rules.

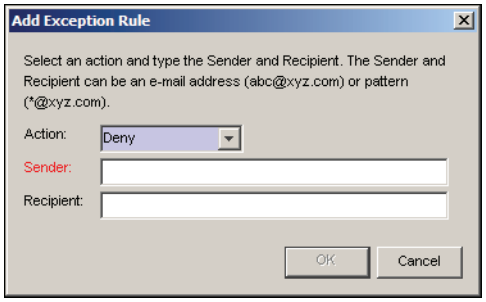
Note

If you have any perimeter firewall between the Firebox that uses spamBlocker and the Internet, it must not block HTTP traffic. The HTTP protocol is used to send requests from the Firebox to the spamBlocker server.

Adding spamBlocker exceptions

At times, the Firebox identifies a message as spam when it is not spam. If you know the address of the sender, you can configure the Firebox with an exception that tells the Firebox not to examine messages from this source address. To look for exceptions, spamBlocker looks at the "mail from:" field. It does not look at the "From:" header that you see in e-mails. If you create an exception rule and it does not operate correctly, make sure you verify that you entered the correct field.

1 From the Exceptions block of the **spamBlocker Configuration** dialog box, click **Add**.
The Add Exception Rule dialog box appears.



2 Select a rule action: **Allow**, **Tag subject**, or **Deny**.

3 Type a sender, recipient, or both. You can type the full e-mail name or use wildcards.

Creating Rules for Bulk and Suspect E-mail on E-mail Clients

Many network administrators allow e-mail that is not confirmed as spam to be delivered to the destined e-mail recipient. They then set up rules in their e-mail client software to have any e-mail tagged as suspect or bulk e-mail put into a special folder on the e-mail client. The procedure below gives instructions on how to configure the Microsoft Outlook e-mail client. For information about how to use this procedure on other types of e-mail clients, look at the user documentation for those products.

Sending spam or bulk e-mail to special folders in Outlook

This procedure shows you the steps to create rules for bulk and suspect e-mail in Microsoft Outlook. You can have e-mail with a "spam" or "bulk" tag delivered directly to special folders in Outlook. When you create these folders, you keep possible spam e-mail out of your usual Outlook folders, but you can get access to the e-mail if it becomes necessary.

If you use another e-mail client, check your user documentation for that product.

Before you start, make sure that you set the action for spam and bulk e-mail to **Add Subject Tag**. You can use the default tags, or create custom tags. The steps below describe how to create folders with the default tags.

1 From your Outlook Inbox, select **Tools > Rules and Alerts**.

2 Click **New Rule** to start the Rules wizard.

3 Select **Start from a blank rule**.

4 Select **Check messages when they arrive**. Click **Next**.

5 Select the condition check box: **when specific words in the subject**. Then, in the bottom pane, edit the rule description by clicking on the specific words. In the **Search Text** dialog box, type the spam tag as *****SPAM*****. If you use a custom tag, type it here instead. Click **Add**. Click **OK**.

6 Click **Next**.

7 The wizard asks what you want to do with the message. Select the **move it to the specified folder** check box. Then, in the bottom pane, click the word **specified** to select the destination folder.

8 In the **Choose a Folder** dialog box, click **New**. In the folder name field, type **Spam**. Click **OK**.

9 Click **Next** two times.

10 To complete the rule setup, type a name for your spam rule. Click **Finish**.

11 Click **Apply**.

12 Repeat these steps to create a rule for bulk e-mail, using the bulk e-mail tag. You can send bulk e-mail to the same folder, or create a separate folder for bulk e-mail.

Reporting False Positives and False Negatives

A false positive e-mail message is a legitimate message that spamBlocker™ incorrectly identifies as spam. A false negative e-mail message is a spam message that spamBlocker does not correctly identify as spam. If you find a false positive or false negative e-mail, you can report the classification error directly to Commtouch. You must have access to the e-mail message to submit the report. To learn how to submit a report for a false positive or false negative, go to:

https://www.watchguard.com/support/advancedfaqs/fw_spam-report.asp

Monitoring spamBlocker Activity

You can use Firebox® System Manager to monitor spamBlocker™ activity.

1 From WatchGuard® System Manager, select the Firebox whose spamBlocker activity you want to monitor.

2 Select **Tools > Firebox System Manager**.

Or,
you can click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

3 From Firebox System Manager, click the **Security Services** tab.
The statistics for spamBlocker appear at the bottom of the screen.

spamBlocker (Activity since last restart)
Messages confirmed as spam: 0
Messages suspected as spam: 0
Messages not spam: 0
Messages marked as bulk email: 0
Messages blocked: 0
Messages tagged: 0
Messages on white/black list: 0

Customizing spamBlocker Using Multiple Proxies

You can configure more than one SMTP Proxy service to use spamBlocker™. This lets you create custom rules for different groups in an organization. For example, you can allow all e-mail to your management and use a spam tag for the marketing team.

If you want to use more than one SMTP Proxy service with spamBlocker, your network must use one of these configurations:

- Each SMTP proxy policy must send e-mail to a different internal e-mail server.

or

- You must set the external source or sources that can send e-mail for each SMTP proxy policy.

Note

spamBlocker does not detect spam in outbound SMTP e-mail.

CHAPTER 25

Using Signature-Based Security Services

Hackers use many methods to attack computers on the Internet. These attacks (called *intrusions* in this chapter) are created to cause damage to your network, get sensitive information, or use your computers to attack other networks.

WatchGuard® offers the Gateway AntiVirus/Intrusion Prevention Service (GAV/IPS) that can identify and stop a possible intrusion. The Intrusion Prevention Service operates with all WatchGuard proxies. WatchGuard Gateway AntiVirus operates with the SMTP, HTTP, and TCP proxies.

When a new intrusion attack is identified, the features that make the virus or attack unique are recorded. These recorded features are known as the signature. GAV/IPS uses these signatures to find viruses and intrusion attacks.

New viruses and intrusion methods appear on the Internet frequently. To make sure that GAV/IPS gives you the best protection, you must update the signatures frequently. You can configure the Firebox® to update the signatures automatically from WatchGuard. You can also update the signatures manually.

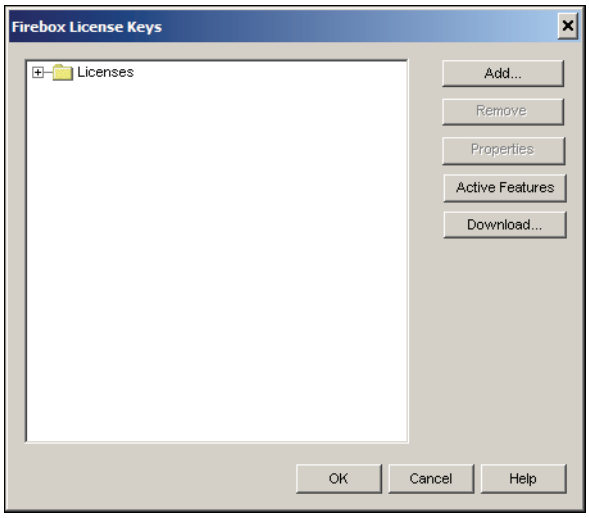
Note

WatchGuard cannot guarantee that the product can stop all viruses or intrusions, or prevent damage to your systems or networks from a virus or intrusion attack.

Installing the Software Licenses

To install Gateway AntiVirus/Intrusion Prevention Service, you must have a license key for each feature.

1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.



2 Click **Add**.

3 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

About Gateway AntiVirus

WatchGuard® Gateway AntiVirus (GAV) stops viruses before they get to computers on your network. GAV operates with the WatchGuard SMTP, HTTP, and TCP proxies. When you enable GAV, the SMTP, HTTP, or TCP proxy looks at e-mail messages and web traffic, and removes any viruses it finds. (The GAV configuration of a TCP policy is in an HTTP proxy action referenced by the TCP proxy action that matches it.)

Note

If your organization does not use an e-mail server protected by the Firebox, Gateway AntiVirus does not protect against e-mail viruses.

If you enable Gateway AntiVirus with the SMTP proxy, it finds viruses encoded with frequently used e-mail attachment methods. These include base64, binary, 7-bit, and 8-bit encoding. Gateway AntiVirus does not find viruses in unencoded or binhex-encoded messages; the Firebox® strips these types of messages.

If you enable Gateway AntiVirus with the HTTP proxy, it finds viruses in web pages that users try to download. If a virus is found, the user's connection is dropped. (GAV does not give a notification about why the connection was dropped.)

Activating Gateway AntiVirus

Before you use Gateway AntiVirus in an SMTP or HTTP proxy policy, you must run the Activate Gateway AntiVirus wizard to activate the feature and create a basic configuration. To do this:

1 From WatchGuard System Manager, select the Firebox that you want to use Gateway AntiVirus.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manager toolbar.

3 From Policy Manager, select **Tasks** > **Gateway AntiVirus** > **Activate**.
The Activate Gateway AntiVirus wizard starts.

4 Click **Next**.

5 Complete the wizard. The wizard shows different screens depending on if you already have proxy policies in your configuration. For example, if you do not, the wizard helps you create a proxy policy. You can then use the wizard again to configure GAV, or see the instructions in the subsequent section. The screens are:

Apply Gateway AntiVirus Settings to your policies

This screen includes a list of proxy policies that are already on your Firebox. From the list, select the proxy policies for which you want to enable Gateway AntiVirus. Any policies that have Gateway AntiVirus already enabled are greyed out.

Create new proxy policies

This screen appears if your Firebox does not yet have policies created for SMTP or HTTP.

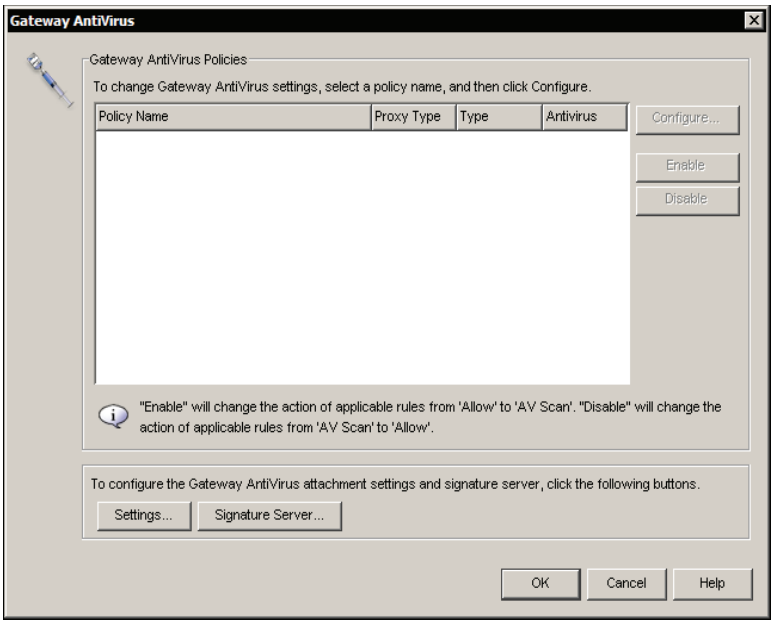
To create a policy, select the corresponding check box. If you select SMTP, enter the mail server IP address.

This wizard creates a default SMTP policy, which is a static NAT policy. To create this default SMTP policy, you must have at least one external interface with a static IP address or PPPoE. Only one policy is created even if you have more than one external interface. The **To** field of the policy is a static NAT entry (the static IP address of the first external interface to the specified mail service IP address). If this default policy does not meet your requirements, you can create an SMTP policy in Policy Manager before you run this wizard.

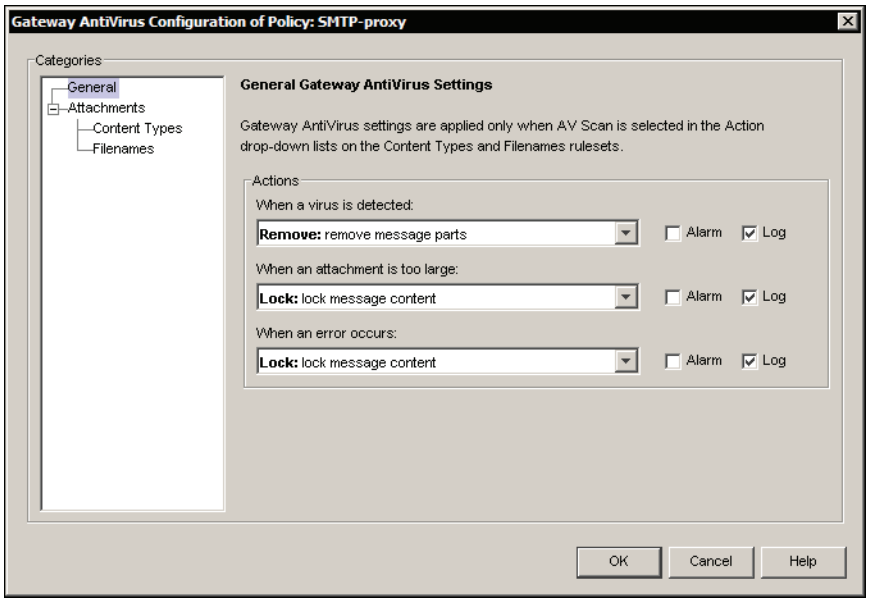
Configuring Gateway AntiVirus

After you use the Activate Gateway AntiVirus wizard to activate GAV and create a basic configuration, you can further refine the configuration.

1 From Policy Manager, select **Tasks** > **Gateway AntiVirus** > **Configure**.
The Gateway AntiVirus dialog box appears, which lists the SMTP, HTTP, and TCP policies that have already been created.


Gateway AntiVirus
Gateway AntiVirus Policies
To change Gateway AntiVirus settings, select a policy name, and then click Configure.
Policy Name
Proxy Type
Type
Antivirus
Configure...
Enable
Disable
"Enable" will change the action of applicable rules from 'Allow' to 'AV Scan'. "Disable" will change the action of applicable rules from 'AV Scan' to 'Allow'.
To configure the Gateway AntiVirus attachment settings and signature server, click the following buttons.
Settings...
Signature Server...
OK
Cancel
Help

2 Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.



3 The fields on this dialog box set the actions necessary if a virus is found in an e-mail message. You also use this dialog box to set actions for when an e-mail message contains an attachment that is

too large or that the Firebox cannot scan. In the **Actions** section, use the drop-down lists to select the Firebox action for each of these conditions:

Allow
Allow the attachment to go to the recipient, even if the content contains a virus.

Drop
Drop the attachment and drop the connection. No information is sent to the source of the message.

Block
Block the attachment, and add the IP address of the sender to the Blocked Sites list.

Additional actions can be applied to the SMTP proxy:

Lock
Lock the attachment. This is a good option for files that are too large for Gateway AntiVirus or that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment.

Remove
Removes the attachment and allows the message through to the recipient.

Note

If you set the configuration to allow attachments, your configuration is less secure.

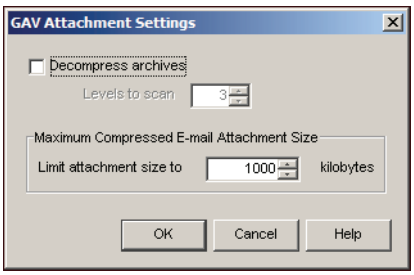
Creating alarms or log entries for antivirus responses

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the General Gateway AntiVirus Settings page to create an alarm for an antivirus response. If you do not want an alarm for an antivirus response, clear the **Alarm** check box for that antivirus response. To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, open the proxy policy for edit. In the proxy action category list, select **Proxy and AV Alarms**.

If you want to record log messages for an antivirus response, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

Configuring GAV engine settings

1 From the **Gateway AntiVirus** dialog box, click **Settings**.



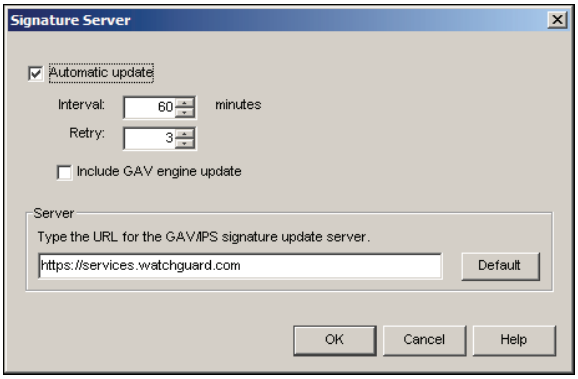
2 To scan inside compressed attachments, select the **Decompress archives** check box. Select or type the number of compression levels to scan.

Compressed attachments that cannot be scanned include encrypted files or files that use a type of compression that we do not support such as password-protected Zip files. Use the Gateway AntiVirus > Configure dialog box to set the action for the Firebox when it finds a message it cannot scan.

3 Enter the maximum file size for e-mail messages in kilobytes.

Configuring the GAV signature server

1 From the **Gateway AntiVirus** dialog box, click **Signature Server**.



2 To enable automatic virus signature updates, select the **Automatic update** check box. Enter the number of minutes between automatic updates.

3 Select the number of retries if the automatic update fails.

4 To update the GAV engine at the same time interval, select the **Include GAV engine update** check box.

5 Do not change the URL of the signature server for GAV/IPS unless you are told to do so by WatchGuard.

6 Click **OK**.

Using Gateway AntiVirus with more than one proxy

You can use more than one SMTP proxy to find and remove viruses for different servers in your organization.

Each proxy that uses Gateway AntiVirus is configured with options that are special to that proxy. For example, you can use different proxy antivirus configurations for e-mail that is for different servers or different destinations. You can strip attachments that are too large to scan for some users, and allow the same attachments for other users.

Unlocking an attachment locked by Gateway AntiVirus

WatchGuard System Manager provides an executable to unlock attachments locked by Gateway AntiVirus:

C:\Program Files\WatchGuard\wsm8\bin\unlock.exe

To open a locked file:

1 Open a command prompt.

2 Type: **Unlock** <path to locked file>

Getting Gateway AntiVirus Status and Updates

You can see the status and get updates for Gateway AntiVirus on the **Security Services** tab in Firebox® System Manager.

Seeing service status

Gateway AntiVirus status shows you whether protection is active. You can also see information about the virus scanner, virus signature versions, and when the signatures were updated.

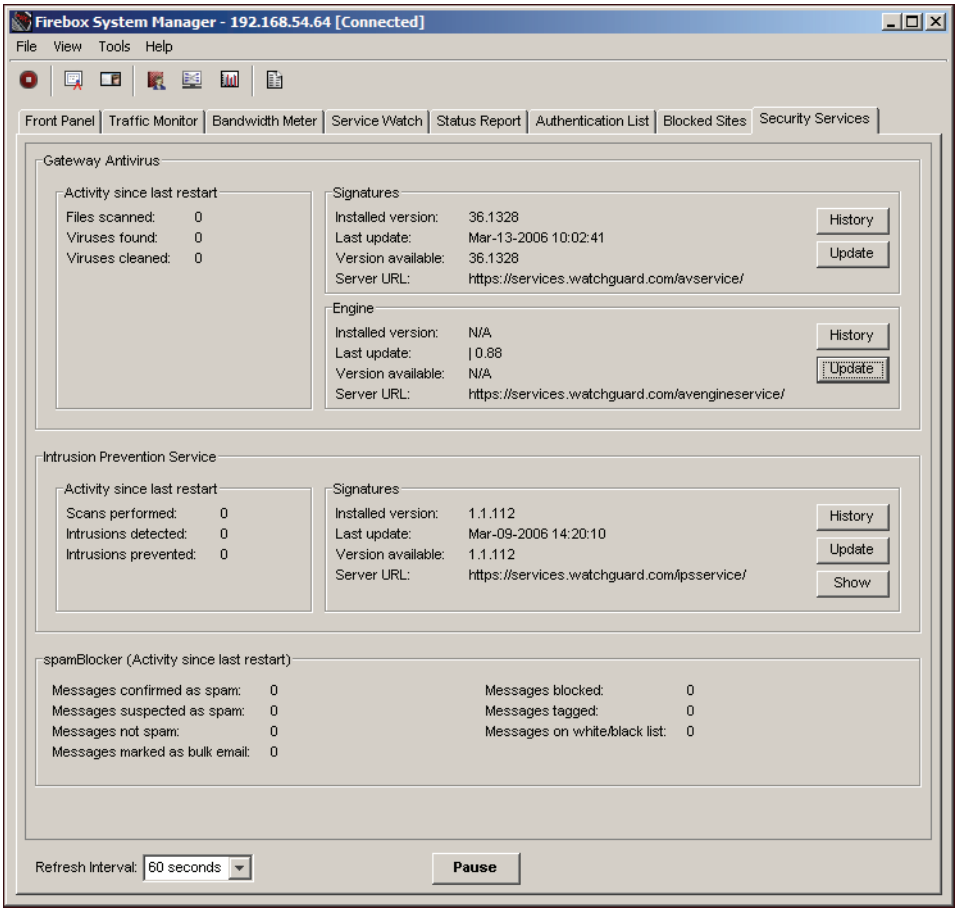
To see service status:

1 From WatchGuard® System Manager, select the Firebox. Select **Tools > Firebox System Manager**.

You can also click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

2 Click the **Security Services** tab.

The window shows the status of the installed security services. Licenses for these features must be installed to see status information.



Updating GAV signatures or the GAV engine manually

Gateway AntiVirus can be configured to update signatures and the GAV engine automatically. You can also update signatures or the GAV engine manually. If the signatures or engine on the Firebox are not current, you are not protected from the latest viruses and attacks. To update the services manually:

1 Start Firebox System Manager.

2 Click the **Security Services** tab.
Security service status appears.

3 Click **Update** for the service you want to update. You must type your configuration passphrase.
The Firebox downloads the most recent available signature update or the most recent available engine for Gateway AntiVirus. You see information about the update in Traffic Monitor.
If no updates are available, the Update button is not active.

Updating the antivirus software

Because there are new types of attacks all the time, you must regularly update your antivirus software. When it is necessary, WatchGuard releases updates to the antivirus database and to the antivirus software. When we release an update, you get an e-mail message from LiveSecurity. You have access to all updates while your Gateway AntiVirus subscription is active.

To download software updates, log in to your LiveSecurity® account at:

www.watchguard.com/support

Activating Intrusion Prevention (IPS)

Hackers use many methods to attack computers on the Internet. The function of these attacks is to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as *intrusions*.

You use Intrusion Prevention Service to find and stop attacks with the WatchGuard proxies. The Firebox® Intrusion Prevention Service examines DNS, FTP, HTTP, and SMTP traffic. It uses the TCP proxy to scan other TCP-based traffic.

Before you use IPS in a proxy policy, you must run the Activate Intrusion Prevention wizard to activate the feature and create a basic configuration. To do this:

1 From WatchGuard System Manager, select the Firebox that will use IPS.

2 Select **Tools > Policy Manager**.

You can also click the Policy Manager icon on the WatchGuard System Manager toolbar.

3 From Policy Manager, select **Tasks > Intrusion Prevention > Activate**.
The Activate Intrusion Prevention wizard starts.

Activate Intrusion Prevention Wizard
Welcome to the
Activate Intrusion Prevention Wizard
Use this wizard to activate Intrusion Prevention (IPS) and create a basic configuration.
Learn more about Intrusion Prevention.
To continue, click Next.
WatchGuard
< Back
Next >
Cancel

4 Click **Next**.

5 Click through the wizard and add the information it asks for. The wizard shows different screens depending on if you already have proxy policies in your configuration. I f you do not, the wizard helps you create a proxy policy. You can then use the wizard again to configure IPS, or see the instructions in the subsequent section. The screens are:

Select proxy policies to enable

This screen shows a list of proxy policies that are already defined on your Firebox. From the list, select the proxy policies you want to enable IPS for. Any policies that have IPS already enabled are grayed out.

Create new proxy policies

This screen shows the proxy types whose corresponding policies do not currently exist. If, for example, you have already created an SMTP policy, it does not appear in the list.

To create a policy, select the corresponding check box. If you select SMTP, enter the mail server IP address. This wizard creates a default SMTP policy, which is a static NAT policy. To create this default SMTP policy, you must have at least one external interface with a static IP address or PPPoE. Only one policy is created even if you have more than one external interface. The **To** field of the policy is a static NAT entry (the static IP address of the first external interface to the specified mail service IP address). If this default policy does not meet your requirements, you can create an SMTP policy in Policy Manager before you run this wizard.

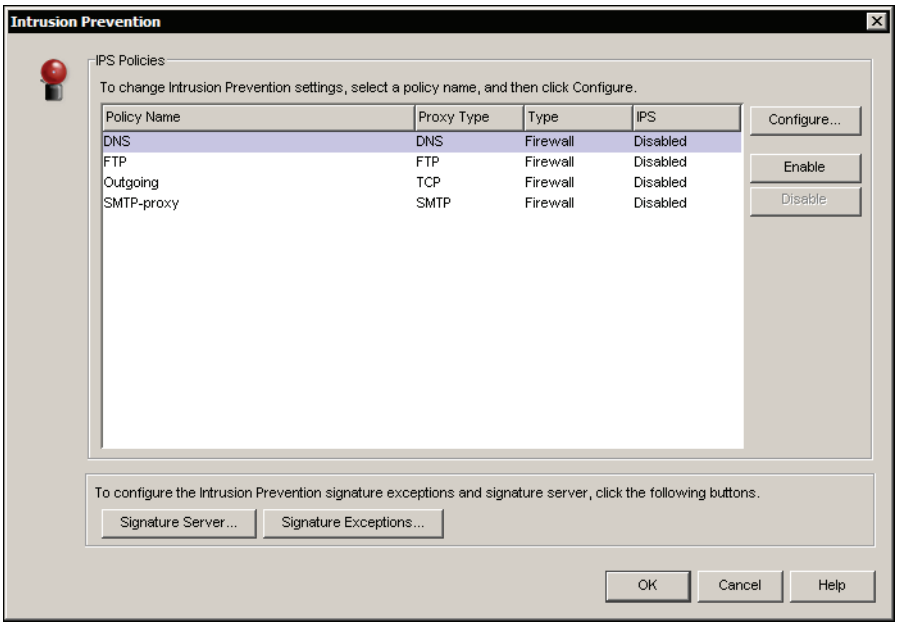
Select Advanced Intrusion Prevention settings (HTTP and TCP only)

If you use the wizard to add an HTTP or TCP policy, you can select protection against Instant Messaging (IM), Peer-to-Peer (P2P), and Spyware.

Configuring Intrusion Prevention

After you use the Activate Intrusion Prevention wizard to activate IPS and create a basic configuration, you can further refine the configuration.

1 From Policy Manager, select **Tasks** > **Intrusion Prevention** > **Configure**.
The Intrusion Prevention dialog box appears, which lists the policies that have already been created.



2 Select the policy you want to configure and click **Configure**.
The General Intrusion Prevention Settings page for that policy appears.

About intrusion severity levels

The proxy settings for intrusion prevention generally use three separate security levels. These three intrusion severity levels look for the following:

High

Vulnerabilities that allow remote access or execution of code, such as buffer overflows, remote command execution, password disclosure, backdoors, and security bypass.

Medium

Vulnerabilities that allow access, disclose server-side source code to attackers, and deny access to legitimate users. Examples are directory traversal, file/source disclosure, DoS, SQL injection, and cross-site scripting.

Low

Vulnerabilities that do not allow the attacker to directly get access, but allow the attacker to get information that can be used in an attack. For example, an attacker can send a command that gets information about the operating system, IP addresses, or topology of a network. Signatures that get access to software applications with vulnerabilities (such as signatures that do not have very specific content) also get this level of severity.

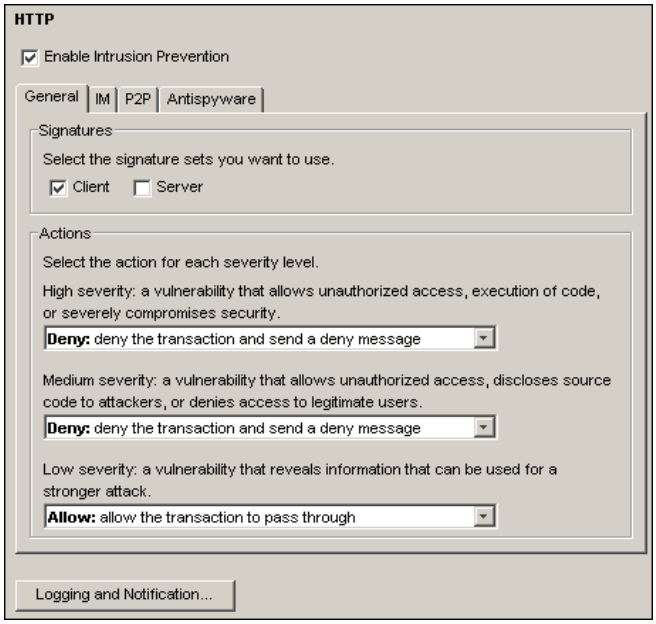
Some signatures that would usually be in the High or Medium level are put in lower levels if their content is not very detailed. They are also put in lower levels if they have a wide scope that could cause false positives.

Configuring intrusion prevention for HTTP or TCP

The HTTP and TCP proxies include options to prevent Instant Messaging (IM), Peer to Peer (P2P), and spyware use.

If you use the TCP proxy and the HTTP proxy, you must be sure to configure actions for IM, P2P, and spyware in the two proxies to apply actions to all IM, P2P, and spyware traffic.

1 Select the **Enable Intrusion Prevention** check box.


HTTP
Enable Intrusion Prevention
General
IM
P2P
Antispyware
Signatures
Select the signature sets you want to use.
Client
Server
Actions
Select the action for each severity level.
High severity: a vulnerability that allows unauthorized access, execution of code, or severely compromises security.
Deny: deny the transaction and send a deny message
Medium severity: a vulnerability that allows unauthorized access, discloses source code to attackers, or denies access to legitimate users.
Deny: deny the transaction and send a deny message
Low severity: a vulnerability that reveals information that can be used for a stronger attack.
Allow: allow the transaction to pass through
Logging and Notification...

2 (HTTP only) Under **Signatures**, click one or both check boxes to use a more accurate list of signatures for HTTP client endpoints, HTTP server endpoints, or both.

3 In the **Actions** section, use the drop-down lists to select the Firebox action for each severity level.

Allow
: You allow a packet so it can get to its recipient, even if the content matches a signature.

Deny
: You deny a packet to stop it and send a TCP reset packet to the sender.

Drop
: You drop a packet to deny it, but send no TCP reset packet to the sender.

Block
: You block a message to drop the packet, and to add the IP address that the packet started from to the Blocked Sites list.

Preventing Instant Messaging (IM) use

The HTTP Proxy has options to prevent Instant Messaging (IM) use. It finds these IM services:

- AOL Instant Messenger (AIM)
- ICQ
- MSN Messenger
- Yahoo Messenger

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **IM** tab.

2 Select the action the Firebox will take when it detects IM: Allow, Drop, Deny, or Block.

3 Select **IM Signature Categories** to enable sets of signatures for different IM services. You can then unselect individual services.

Preventing Peer to Peer (P2P) use

The HTTP Proxy has options to prevent Peer to Peer (P2P) use. It finds these types of P2P services:

- BitTorrent
- eDonkey2000 (ed2k)
- GNUtella
- Kazaa
- Napster
- Phatbot

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **P2P** tab.

2 Select the action the Firebox will take when it detects IM: Allow, Drop, Deny, or Block.

3 Select **P2P Signature Categories** to enable sets of signatures for different P2P services. You can then unselect individual services.

Blocking spyware

The HTTP and TCP proxies provide these antispyware categories:

Adware
: A software application in which advertising banners are shown while the program is in operation. It sometimes includes code that records a user's personal information and sends it to third parties, without the user's authorization or knowledge.

Dialer
: A software application that can hijack a user's modem and dial toll numbers that get access to inappropriate web sites.

Downloader
: A program that gets and installs other files. Most are configured to get files from a designated web or FTP site.

Hijacker
: A type of malware program that changes your computer's browser settings and redirects you to web sites that you did not plan to browse to.

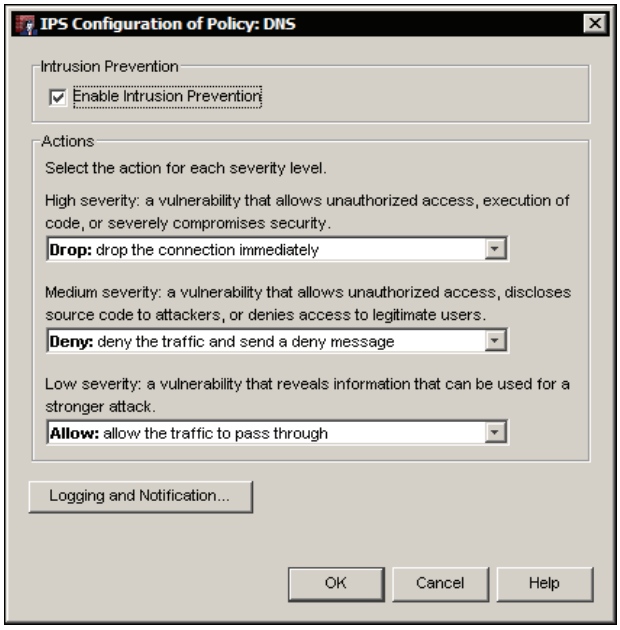
Trackware
: Any software that uses a computer's Internet connection to send personal information without the user's permission.

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **Antispyware** tab.

2 Select the action the Firebox will take when it detects spyware: Allow, Drop, Deny, or Block.

Configuring Intrusion Prevention for FTP, SMTP, or DNS

1 Select the **Enable Intrusion Prevention** check box.


IPS Configuration of Policy: DNS
Intrusion Prevention
Enable Intrusion Prevention
Actions
Select the action for each severity level.
High severity: a vulnerability that allows unauthorized access, execution of code, or severely compromises security.
Drop: drop the connection immediately
Medium severity: a vulnerability that allows unauthorized access, discloses source code to attackers, or denies access to legitimate users.
Deny: deny the traffic and send a deny message
Low severity: a vulnerability that reveals information that can be used for a stronger attack.
Allow: allow the traffic to pass through
Logging and Notification...
OK
Cancel
Help

2 For each severity level, select one of the following actions.

Allow

Allow the attachment.

Deny

Deny the attachment and send a deny message to the sender.

Drop

Drop the attachment to stop the message and drop the connection. No information is sent to the source of the message.

Block

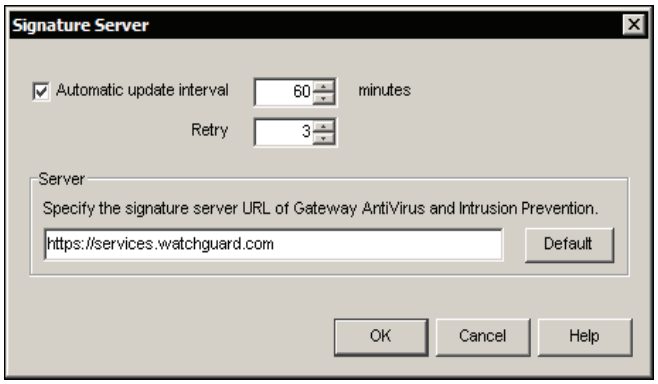
Block a message to drop the attachment, and to add the IP address of the sender to the Blocked Sites list.

Note

If you set the configuration to allow attachments, your configuration is less secure.

Configuring the signature server

1 From the **Intrusion Prevention** dialog box, click **Signature Server**.



2 To enable automatic virus signature updates, select the **Automatic update** check box. Enter the number of minutes between automatic updates.

3 Select the number of retries if the automatic update fails.

4 Type the URL of the signature server for GAV/IPS.

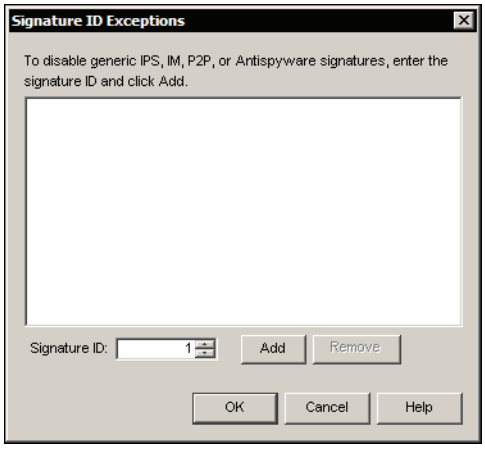
5 Click **OK**.

6 Select **File > Save > To Firebox**.

7 Type your configuration passphrase and click **OK**.

Configuring signature exceptions

1 From the **Intrusion Prevention** dialog box, click **Signature Exceptions**.
The Signature ID Exceptions dialog box appears.



2 Type any generic IPS, IM, P2P or Antispyware signatures that you want to disable. Click **Add**.

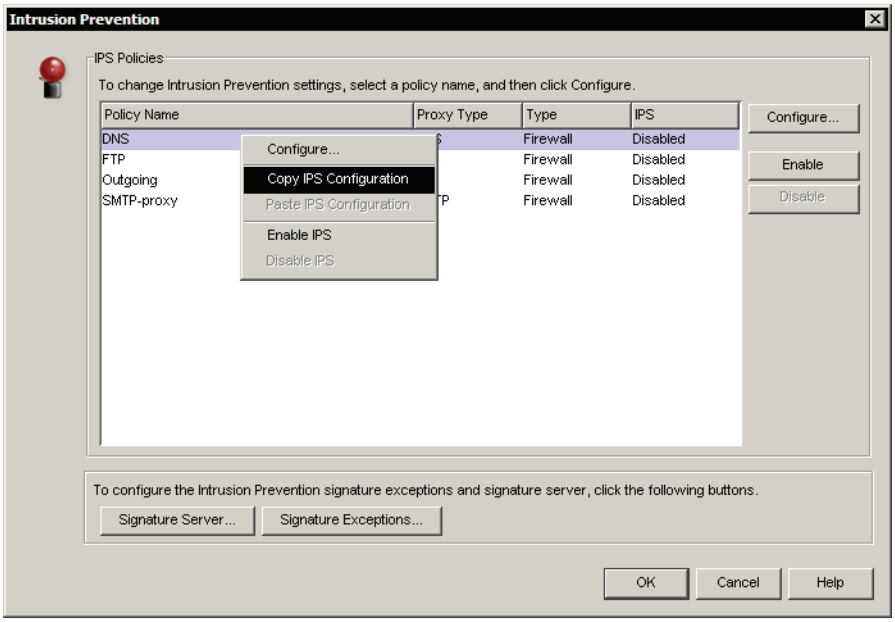
Copying IPS settings to other policies

After configuring IPS for one proxy, you can copy the same configuration to other proxies. However, you can copy IPS settings only between policies with compatible IPS configurations.

- Between FTP, DNS, and SMTP policies

- Between multiple TCP policies
- Between multiple HTTP policies

1 From the **Intrusion Prevention** dialog box, select the proxy whose configuration you want to copy, right-click, and select **Copy IPS Configuration**.



2 From the same dialog box, select the proxy or proxies you want to copy the configuration to, right-click, and select **Paste IPS Configuration**.

Getting Intrusion Prevention Service Status and Updates

You can see the status and get updates for Intrusion Prevention Service on the **Security Services** tab in Firebox® System Manager.

Seeing service status

Intrusion Prevention Service status shows you whether protection is active. You can also see information about the signature versions.

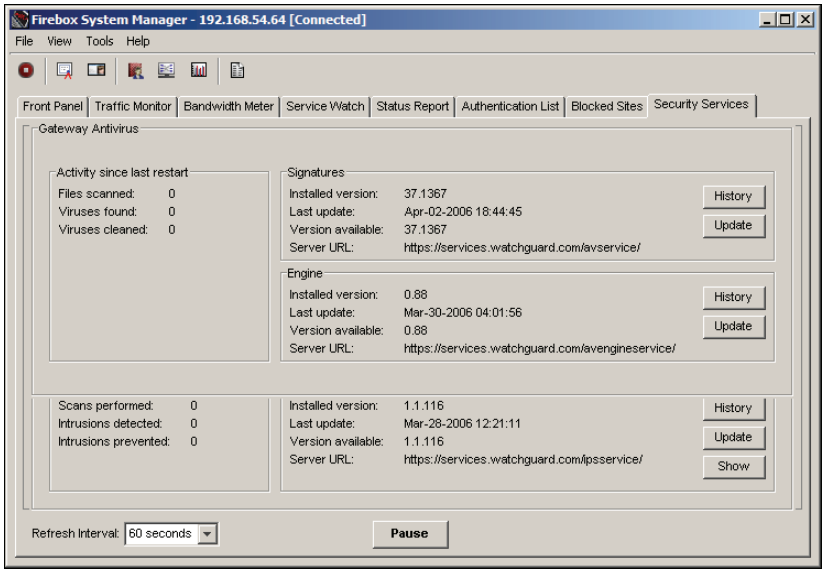
To see service status:

1 From WatchGuard® System Manager, select the Firebox. Select **Tools > Firebox System Manager**.

You can also click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

2 Click the **Security Services** tab.

The window shows the status for the installed security services. Licenses for these features must be installed to see status information.



3 Click **History** to see the date, version, and status of the signature updates that have occurred.

Updating signatures manually

Intrusion Prevention Service can be configured to update signatures automatically. You can also update signatures manually. If the signatures are not current, you are not protected from the latest viruses and attacks.

To update the services manually:

1 Start Firebox System Manager.

2 Click the **Security Services** tab.

Security service status appears.

3 Click **Update** for the service to update.

The Firebox downloads the most recent available signature update. You see information about the update in Traffic Monitor.

If there are no updates available, the Update button is not active.

CHAPTER 26

Advanced Networking

Note

Most of the advanced networking features described in this chapter—Quality of Service and the OSPF and BGP dynamic routing protocols—are available only in Fireware® Pro. Only the RIP dynamic routing protocol is available with Fireware.

Advanced networking features are designed to give the Firebox® administrator more control and greater efficiency with a very large or high-traffic network. These features include:

Quality of Service (QoS)
: Fireware's QoS feature lets you set priority queues, bandwidth restrictions, and connection rate limits on individual policies.

Dynamic routing
: In addition to static routing, the Firebox can use the dynamic routing protocols RIP versions 1 and 2, OSPF version 2, and BGP version 4. These routing protocols allow for the dynamic modifying of routing tables.

Creating QoS Actions

Note

This feature is available only in Fireware® Pro.

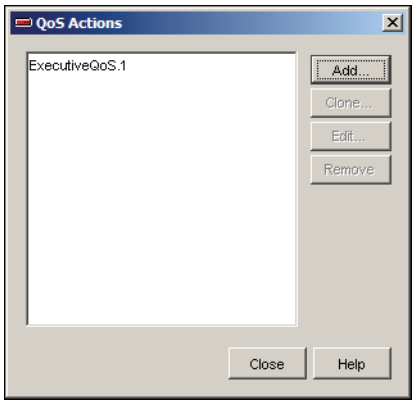
In a large network with many host computers, the volume of data that moves through the firewall can be very large. When the traffic is too much for the network, data packets are dropped. A network administrator can prevent data loss for important business applications with Quality of Service (QoS). For example, you can assign traffic such as data exchanges between corporate and branch offices a higher priority than low-priority traffic such as web surfing or browsing.

With Fireware® Pro, you can set Quality of Service (QoS) actions and apply them to policies to make sure that bandwidth for important traffic is always available.

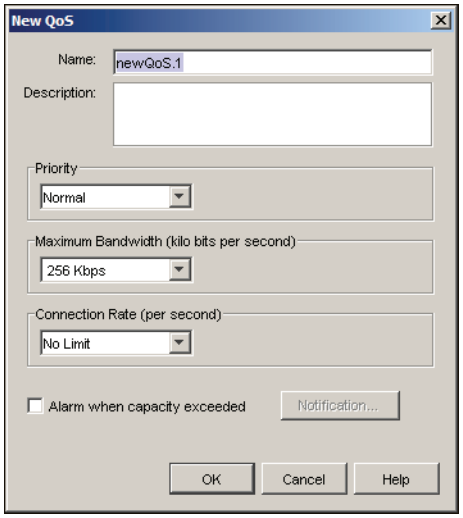
You can also define an alarm to occur when network capacity is exceeded according to the QoS action's parameters. You can configure the alarm to make the Firebox® send an event notification to the SNMP

management system, or to send a notification in the form of e-mail or a pop-up window on the management station.

1 From Policy Manager, select **Setup > Actions > QoS**.
The QoS Actions dialog box appears.



2 Click **Add**.
The New QoS dialog box appears.



3 Type the name and description of the QoS action.

4 Set **Priority** to normal or high to give traffic priority treatment.
These categories are often known as queues.

5 Use the **Maximum Bandwidth** drop-down list to set or remove the bandwidth limits for this action.
Use No Limits to remove bandwidth restrictions for important traffic, or select a maximum kilobytes per second bandwidth. When the maximum bandwidth limit is reached, the QoS action starts.

6 Use the **Connection Rate** drop-down list to set a maximum number of connections per second that can occur before QoS actions start.
The default configuration puts no limits on the connection rate. If you select Custom, you can type the maximum connection rate. When this limit is reached, the QoS action starts.

7 If you want to set an alarm when the bandwidth or connection rate is exceeded, select the **Alarm when capacity exceeded** check box. Use this alarm to determine if a policy requires more bandwidth. Click **Notification** and set the notification parameters, as described in “Setting logging and notification parameters” on page 129.

8 Click **OK**.
The new action appears in the QoS Actions dialog box.

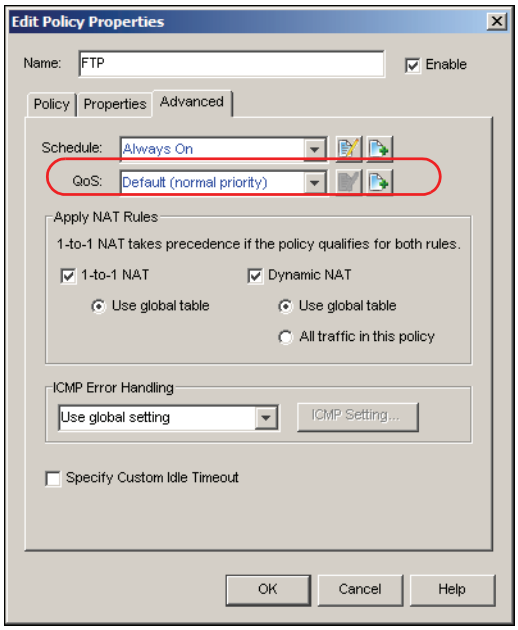
Applying QoS actions to policies

After you have created QoS actions, you can apply them to the policies you have configured in Policy Manager. To apply a QoS action:

1 From Policy Manager, double-click on the policy to which you want to add a QoS action.

2 Select the **Advanced** tab.

3 From the **QoS** drop-down list, select the QoS action to apply to the policy.



4 Use the **View/Edit** or **New/Clone** buttons (at the right of the **Schedule** and **QoS** fields) to change the properties of the QoS action or to create a new QoS action for the policy.

5 Click **OK**. Save your changes to the Firebox.

Using QoS in a multiple WAN environment

When a QoS action is applied on a multiple WAN policy with multiple WAN set up in round robin mode, the maximum bandwidth and connection rate settings in the QoS action control the total throughput and connection rate across all interfaces. This includes all external interfaces that are configured to route traffic. This also includes external interfaces that are down.

When a QoS action is applied on a multiple WAN policy with multiple WAN set up in WAN failover mode, the maximum bandwidth and connection rate settings in the QoS action control the throughput and connection rate across the one external interface that is currently sending packets.

Dynamic Routing

A routing protocol is the language a router speaks with other routers to share information about the status of network routing tables. With static routing, routing tables are set and do not change. If a router on the remote path fails, a packet cannot get to its destination.

Dynamic routing lets routing tables in routers change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Fireware® Pro supports RIP v1 and v2, OSPF, and BGP v4 dynamic routing protocols. Fireware supports only RIP v1 and v2.

Routing daemon configuration files

To use any of the dynamic routing protocols with Fireware, you must import or type a dynamic routing configuration file for the routing daemon you choose. This configuration file includes information such as a password and log file name. You can find configuration templates for each of the routing protocols in this FAQ:

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

You can find a list of supported configuration commands for each routing protocol in the sections below. The command sections below appear in the order they must go in an operating configuration file.

Notes about configuration files:

- The "!" and the "#" characters are comment characters. If the first character of the word is one of the comment characters, then the rest of the line is interpreted as a comment. If the comment character is not the first character of the word, it is interpreted as a command.
- Usually, you can use the word "no" at the beginning of the line to disable a command. For example: "no network 10.0.0.0/24 area 0.0.0.0" disables the backbone area on the specified network.

Using RIP

Note

Support for this protocol is available in both Fireware® and Fireware Pro.

RIP (Routing Information Protocol) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, in turn, sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. OSPF is a better alternative for larger networks.

RIP Version 1

RIP V1 uses a UDP broadcast over port 520 to send updates to routing tables. To create or modify a routing configuration file, here is a table of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample RIP configuration file found in this FAQ:

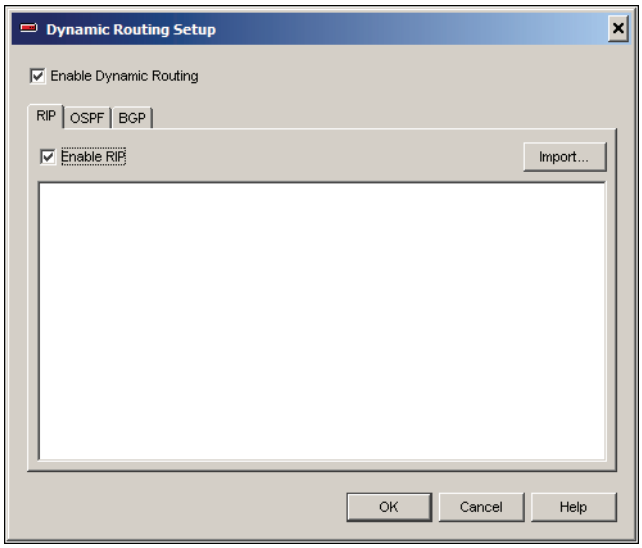
https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

Section	Command	Description
Set simple password or MD5 authentication on an interface		
	interface eth[N]	Begin section to set authentication type for interface
	ip rip authentication string [PASSWORD]	Set RIP authentication password
	key chain [KEY-CHAIN]	Set MD5 key chain name
	key [INTEGER]	Set MD5 key number
	key-string [AUTH-KEY]	Set MD5 authentication key
	interface eth[N]	Begin section to set authentication type for interface
	ip rip authentication mode md5	Use MD5 authentication
	ip rip authentication mode key-chain [KEY-CHAIN]	Set MD5 authentication key-chain
Configure RIP routing daemon		
	router rip	Enable RIP daemon
	version [1|2]	Set RIP version to 1 or 2 (default version 2)
	ip rip send version [1|2]	Set RIP to send version 1 or 2
	ip rip receive version [1|2]	Set RIP to receive version 1 or 2
	no ip split-horizon	Disable split-horizon; enabled by default
Configure interfaces and networks		
	no network eth[N]	
	passive-interface eth[N]	
	passive-interface default	
	network [A.B.C.D/M]	
	neighbor [A.B.C.D/M]	
Distribute routes to RIP peers and inject OSPF or BGP routes to RIP routing table		
	default-information originate	Share route of last resort (default route) with RIP peers
	redistribute kernel	Redistribute firewall static routes to RIP peers
	redistribute connected	Redistribute routes from all interfaces to RIP peers
	redistribute connected route-map [MAPNAME]	Redistribute routes from all interfaces to RIP peers, with a route map filter (mapname)
	redistribute ospf	Redistribute routes from OSPF to RIP
	redistribute ospf route-map [MAPNAME]	Redistribute routes from OSPF to RIP, with a route map filter (mapname)
	redistribute bgp	Redistribute routes from BGP to RIP
	redistribute bgp route-map [MAPNAME]	Redistribute routes from BGP to RIP, with a route map filter (mapname)
Configure route redistribution filters with route maps and access lists		

Section	Command	Description
	access-list [PERMIT | DENY] [LISTNAME] [A.B.C.D/M | ANY]	Create an access list to allow or deny redistribution of only one IP address or for all IP addresses
	route-map [MAPNAME] permit [N]	Create a route map with a name and allow with a priority of N
	match ip address [LISTNAME]	

Configuring Fireware or Fireware Pro to use RIP v1

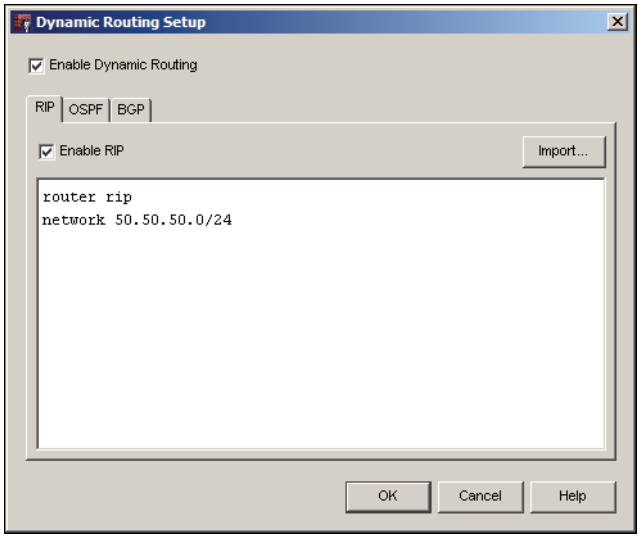
1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click **Enable Dynamic Routing** and **Enable RIP**.

3 Click **Import** to import a routing daemon configuration file, or type your configuration file in the text box.

If you click Import, you can browse to the location of the RIP daemon configuration template. It is located in C:\Documents and Settings\My Documents\My WatchGuard.



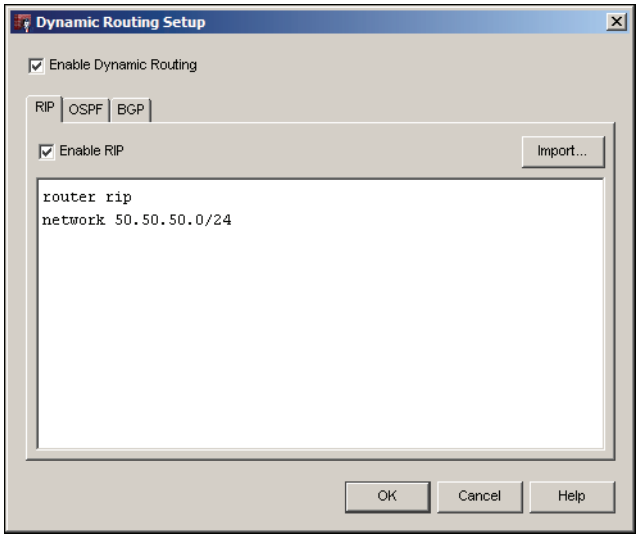
4 Click **OK**.

Allowing RIP v1 traffic through the Firebox

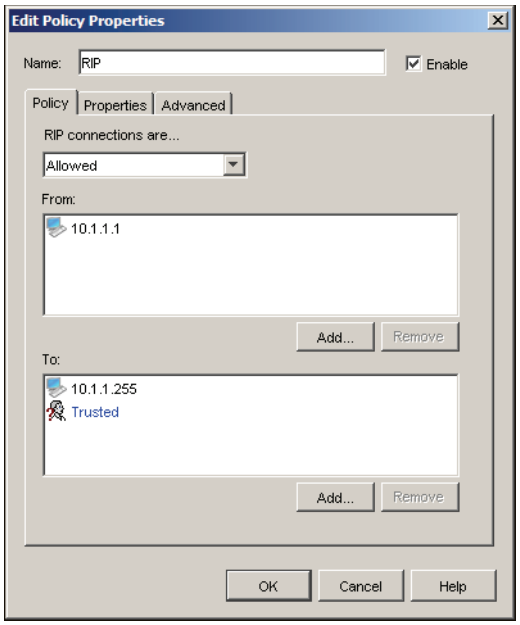
You must add and configure a policy to allow RIP broadcasts from the router to the network broadcast IP address. You must also add the IP address of the Firebox® interface to the **To** field.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**.

The New Policy Properties window appears for RIP.



2 In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the Firebox® interface it connects to. You must also add the network broadcast IP address.



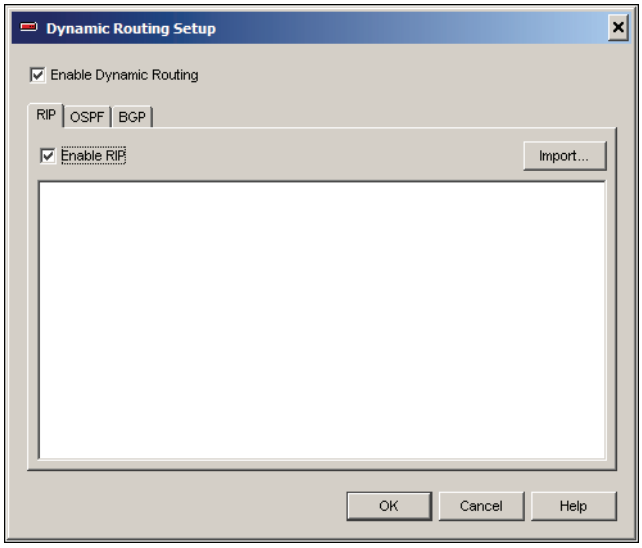
3 Click **OK**.

RIP Version 2

RIP v2 uses multicast to send routing table updates. To create or modify a routing configuration file, refer to the table of supported RIP routing commands in the section *RIP Version 1*. Any command that uses a network IP address must include the subnet mask or RIP v2 will not operate. The sections must appear in the configuration file in the same order they appear in this table.

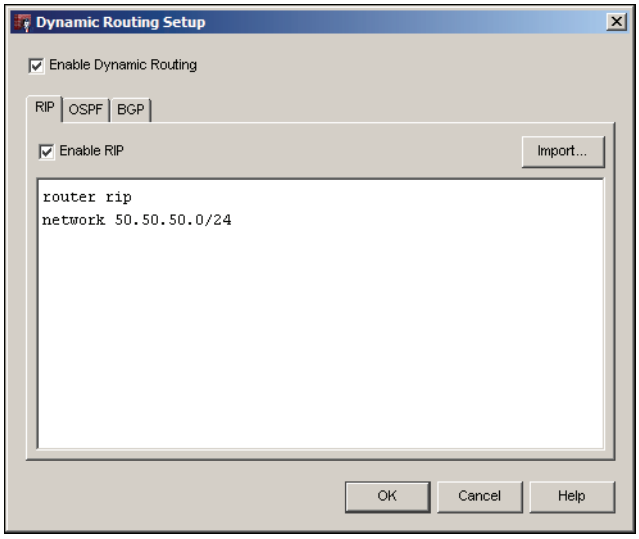
Configuring Fireware to use RIP v2

1 In Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click **Enable Dynamic Routing** and **Enable RIP**.

3 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.
If you click Import, you can browse to the location of the RIP daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.



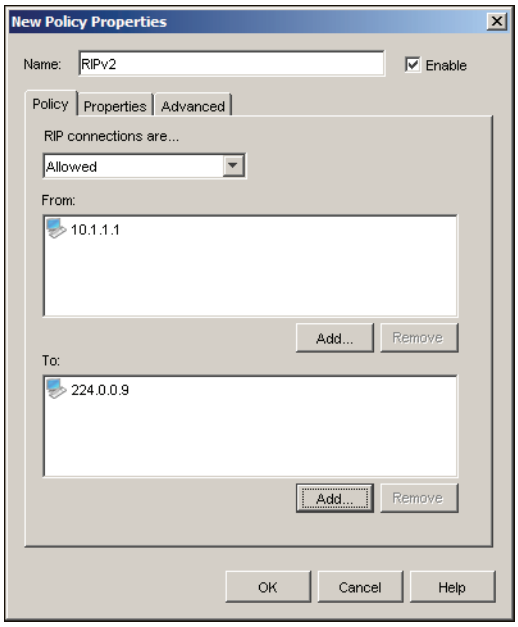
4 Click **OK**.

Allowing RIP v2 traffic through the Firebox

You must add and configure a policy to allow RIP v2 multicasts from the routers that have RIP v2 enabled to the reserved multicast IP address for RIP v2.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**.
The New Policy Properties window appears for RIP.

2 In the **New Policy Properties** window, configure the policy to allow traffic from the IP or network address of the router using RIP to the multicast address 224.0.0.9.



3 Click **OK**.

Using OSPF

Note

Support for this protocol is available only in Fireware® Pro.

OSPF (Open Shortest Path First) is an interior router protocol used in larger networks. With OSPF, a router that sees a change to its routing table or that detects a change in the network immediately sends a multicast update to all other routers in the network. OSPF is different than RIP because:

- OSPF sends only the part of the routing table that has changed in its transmission. RIP sends the full routing table each time.
- OSPF sends a multicast only when its information has changed. RIP sends the routing table every 30 seconds.

There are also a few specific things it is important to understand about OSFP:

- If you have more than one OSPF area, one area must be area 0.0.0.0 (the backbone area).
- All areas must be adjacent to the backbone area. If they are not, you must configure a virtual link to the backbone area.

OSPF daemon configuration

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample OSPF configuration file found in this FAQ:

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

Section	Command	Description
Configure Interface		
	ip ospf authentication-key [PASSWORD]	Set OSPF authentication password
	interface eth[N]	Begin section to set properties for interface
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Set MD5 authentication key ID and key
	ip ospf cost [1-65535]	Set link cost for the interface (see OSP Interface Cost table below)
	ip ospf hello-interval [1-65535]	Set interval to send hello packets; default is 10 seconds
	ip ospf dead-interval [1-65535]	Set interval after last hello from a neighbor before declaring it down; default is 40 seconds
	ip ospf retransmit-interval [1-65535]	Set interval between link-state advertisements (LSA) retransmissions; default is 5 seconds
	ip ospf transmit-delay [1-3600]	Set time required to send LSA update; default is 1 second
	ip ospf priority [0-255]	Set router priority; high value increases eligibility to become the designated router (DR)
Configure OSPF Routing Daemon		
	router ospf	Enable OSPF daemon
	ospf router-id [A.B.C.D]	Set router ID for OSPF manually; router will determine its own ID if not set
	ospf rfc 1583compatibility	Enable RFC 1583 compatibility (can lead to routing loops)
	ospf abr-type [cisco|ibm|shortcut|standard]	More information about this command can be found in draft-ietf-abr-alt-o5.txt
	passive interface eth[N]	Disable OSPF announcement on interface eth[N]
	auto-cost reference bandwidth [0-429495]	Set global cost (see OSPF cost table below); do not use with "ip ospf [COST]" command
	timers spf [0-4294967295][0-4294967295]	Set OSPF schedule delay and hold time
Enable OSPF on a Network *The "Area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	network [A.B.C.D/M] area [Z]	Announce OSPF on network A.B.C.D/M for area 0.0.0.Z
Configure Properties for Backbone Area or Other Areas *The "Area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	area [Z] range [A.B.C.D/M]	Create area 0.0.0.Z and set a classful network for the area (range and interface network and mask settings should match)
	area [Z] virtual-link [W.X.Y.Z]	Set virtual link neighbor for area 0.0.0.Z

Section	Command	Description
	area [Z] stub	Set area 0.0.0.Z as a stub
	area [Z] stub no-summary	
	area [Z] authentication	Enable simple password authentication for area 0.0.0.Z
	area [Z] authentication message-digest	Enable MD5 authentication for area 0.0.0.Z
Redistribute OSPF Routes		
	default-information originate	Share route of last resort (default route) with OSPF
	default-information originate metrics [0-16777214]	Share route of last resort (default route) with OSPF
	default-information originate always	Share route of last resort (default route) with OSPF
	default-information originate always metrics [0-16777214]	Share route of last resort (default route) with OSPF
	redistribute connected	Redistribute routes from all interfaces to OSPF
	redistribute connected metrics	Redistribute routes from all interfaces to OSPF
Configure Route Redistribution with Access Lists and Route Maps		
	access-list [LISTNAME] permit [A.B.C.D/M]	Create an access list to allow distribution of A.B.C.D/M
	access-list [LISTNAME] deny any	Restrict distribution of any route map not specified above
	route-map [MAPNAME] permit [N]	Create a route map with name [MAPNAME] and allow with a priority of [N]
	match ip address [LISTNAME]	

OSPF Interface Cost table

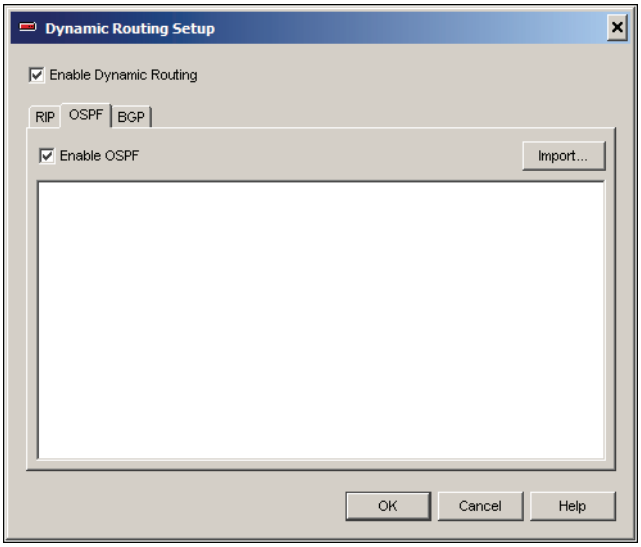
The OSPF protocol finds the most efficient route between two points. To do this, it looks at factors such as interface link speed, the number of hops between points, and other metrics. By default, OSPF uses the actual link speed of a device to calculate the total cost of a route. You can set the interface cost manually to help maximize efficiency if, for example, your gigabyte-based firewall is connected to a 100M router. Use the numbers in the OSPF Interface Cost table to manually set the interface cost to a value different than the actual interface cost.

Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Ethernet	1G	100M	1
Ethernet	100M	10M	10
Ethernet	10M	1M	100
Modem	2M	200K	500
Modem	1M	100K	1000
Modem	500K	50K	2000
Modem	250K	25K	4000
Modem	125K	12500	8000

Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Modem	62500	6250	16000
Serial	115200	9216	10850
Serial	57600	4608	21700
Serial	38400	3072	32550
Serial	19200	1636	61120
Serial	9600	768	65535

Configuring Fireware Pro to use OSPF

1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.

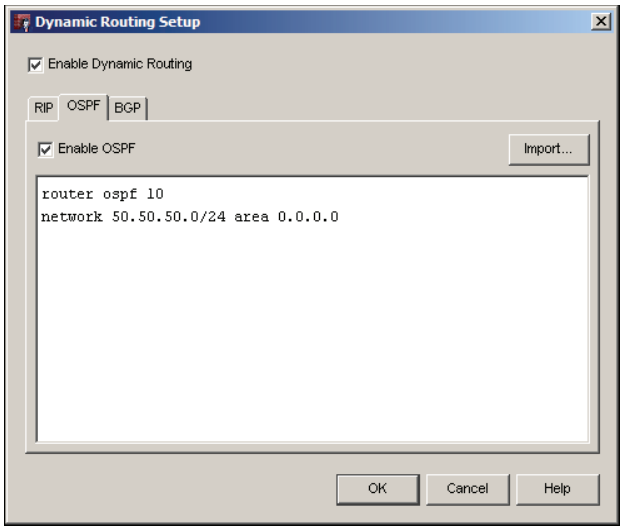


2 Click the **OSPF** tab.

3 Click **Enable Dynamic Routing** and **Enable OSPF**.

4 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.

If you click Import, you can browse to the location of the OSPF daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.



5 Click **OK**.

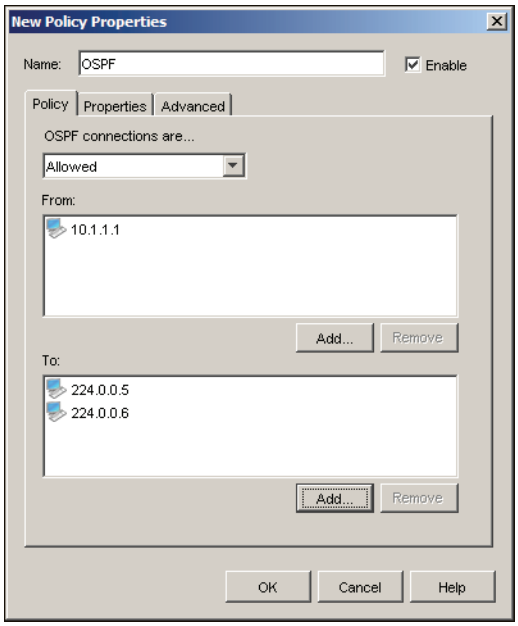
Allowing OSPF traffic through the Firebox

You must add and configure a policy to allow OSPF multicasts from the routers that have OSPF enabled to the reserved multicast addresses for OSPF.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **OSPF**. Click **Add**.

The New Policy Properties window appears for OSPF.

2 In the **New Policy Properties** window, configure the policy to allow traffic from the IP or network address of the router using OSPF to the IP addresses 224.0.0.5 and 224.0.0.6. Click **OK**.



Using BGP

Note

Support for this protocol is available only in Fireware® Pro.

Border Gateway Protocol (BGP) is a scalable dynamic routing protocol used by groups of routers to share routing information. BGP is the routing protocol used on the Internet. BGP uses route parameters or "attributes" to define routing policies and create a stable routing environment. BGP allows you to advertise more than one path to and from the Internet to your network and resources. This gives you redundant paths and can increase your uptime.

Hosts using BGP use TCP to send updated routing table information when one host finds a change. The host sends only the part of the routing table that has the change. BGP uses classless interdomain routing (CIDR) to reduce the size of the Internet routing tables. The size of the BGP routing table in Fireware® Pro is set at 32K.

The size of the typical WatchGuard® customer wide area network (WAN) is best suited for OSPF dynamic routing. A WAN can also use external border gateway protocol (EBGP) when more than one gateway to the Internet is available. EBGP allows you to take full advantage of the redundancy possible with a multi-homed network.

To participate in EBGP with an ISP you must have an autonomous system number (ASN). You must get an ASN from one of the regional registries in the table below. After you are assigned your own ASN you must contact each ISP to get their AS numbers and other necessary information.

Region	Registry Name	Web Site
North America	ARIN	www.arin.net
Europe	RIPE NCC	www.ripe.net
Asia Pacific	APNIC	www.apnic.net
Latin America	LACNIC	www.lacnic.net
Africa	AfriNIC	www.afrinic.net

BGP daemon configuration

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample BGP configuration file found in this FAQ:

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

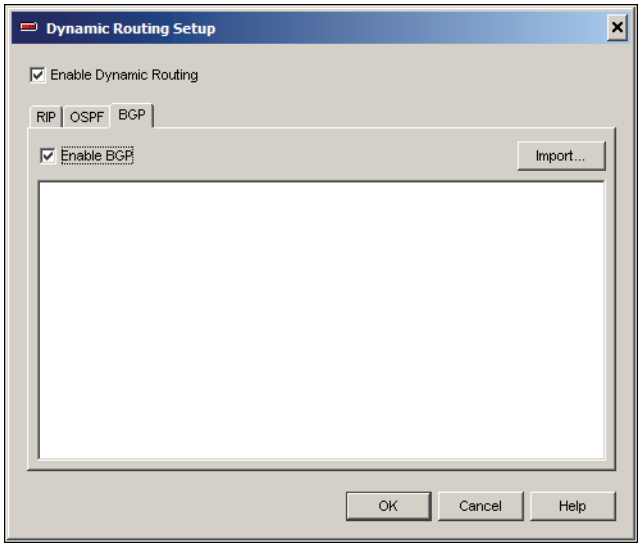
Do not use BGP configuration parameters that you do not get from your ISP.

Section	Command	Description
Configure BGP Routing Daemon		
	router bgp [ASN]	Enable BGP daemon and set autonomous system number (ASN); this is supplied by your ISP
	network [A.B.C.D/M]	Announce BGP on network A.B.C.D/M
	no network [A.B.C.D/M]	Disable BGP announcements on network A.B.C.D/M
Set Neighbor Properties		
	neighbor [A.B.C.D] remote-as [ASN]	Set neighbor as member of remote ASN
	neighbor [A.B.C.D] ebgp-multihop	Set neighbor on another network using EBGP multi-hop
	neighbor [A.B.C.D] version 4+	Set BGP version (4, 4+, 4-) for communication with neighbor; default is 4
	neighbor [A.B.C.D] update-source [WORD]	Set the BGP session to use a specific interface for TCP connections
	neighbor [A.B.C.D] default-originate	Announce default route to BGP neighbor [A.B.C.D]
	neighbor [A.B.C.D] port 189	Set custom TCP port to communicate with BGP neighbor [A.B.C.D]
	neighbor [A.B.C.D] send-community	Set peer send-community
	neighbor [A.B.C.D] weight 1000	Set a default weight for neighbor's [A.B.C.D] routes
	neighbor [A.B.C.D] maximum-prefix [NUMBER]	Set maximum number of prefixes allowed from this neighbor
Community Lists		

Section	Command	Description
	ip community-list [<1-99>|<100-199>] permit AA:NN	Specify community to accept autonomous system number and network number separated by a colon
Peer Filtering		
	neighbor [A.B.C.D] distribute-list [LISTNAME] [IN|OUT]	Set distribute list and direction for peer
	neighbor [A.B.C.D] prefix-list [LISTNAME] [IN|OUT]	To apply a prefix list to be matched to incoming advertisements or outgoing advertisements to that neighbor
	neighbor [A.B.C.D] filter-list [LISTNAME] [IN|OUT]	To match an autonomous system path access list to incoming routes or outgoing routes
	neighbor [A.B.C.D] route-map [MAPNAME] [IN|OUT]	To apply a route map to incoming or outgoing routes
Redistribute Routes to BGP		
	redistribute kernel	Redistribute static routes to BGP
	redistribute rip	Redistribute RIP routes to BGP
	redistribute ospf	Redistribute OSPF routes to BGP
Route Reflection		
	bgp cluster-id A.B.C.D	To configure the cluster ID if the BGP cluster has more than one route reflector
	neighbor [W.X.Y.Z] route-reflector-client	To configure the router as a BGP route reflector and configure the specified neighbor as its client
Access Lists and IP Prefix Lists		
	ip prefix-list PRELIST permit A.B.C.D/E	Set prefix list
	access-list NAME [deny|allow] A.B.C.D/E	Set access list
	route-map [MAPNAME] permit [N]	In conjunction with the “match” and “set” commands, this defines the conditions and actions for redistributing routes
	match ip address prefix-list [LISTNAME]	Matches the specified access_list
	set community [A:B]	Set the BGP community attribute
	match community [N]	Matches the specified community_list
	set local-preference [N]	Sets the preference value for the autonomous system path

Configuring Fireware Pro to use BGP

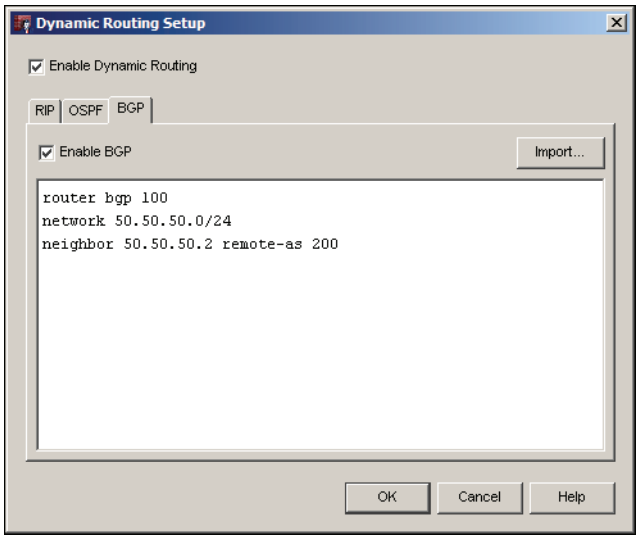
1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click the **BGP** tab.

3 Click **Enable Dynamic Routing** and **Enable BGP**.

4 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.
If you click Import, you can browse to the location of the BGP daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.



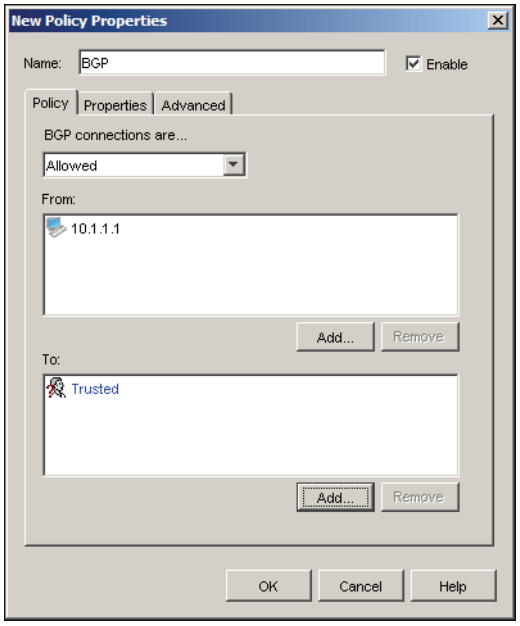
5 Click **Select a BGP Configuration** file. Click **OK**.

Allowing BGP traffic through the Firebox

You must add and configure a policy to allow BGP traffic to the Firebox® from the approved networks. These networks must be the same networks you defined in your BGP configuration file.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **BGP**. Click **Add**.
The New Policy Properties window appears for BGP.

2 In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router using BGP to the Firebox interface it connects to. Click **OK**.



CHAPTER 27

High Availability

Note

High Availability is available only in Fireware® Pro.

High Availability (HA) refers to the ability of a network to operate when hardware or software fails. When you add redundancy to your network, you remove one point of vulnerability.

The WatchGuard® High Availability feature enables the installation of two Firebox® devices in a failover configuration. The configuration includes one Firebox we identify as the primary device and the other we identify as the secondary device. One of these devices is always in active mode and the other in standby mode. These two Fireboxes are known as "peers." They constantly send messages to each other to communicate their status.

When a failover event occurs, the standby system becomes active. After a Firebox becomes active, it stays active until it goes offline and the standby Firebox starts as the active unit.

This chapter includes two methods to configure High Availability. Use the first method if the Firebox devices to configure for High Availability are Firebox X Core or Peak e-Series devices. If the two Firebox devices are Firebox X Core or Peak devices and not e-Series appliances, you can use the first or second method.

High Availability Requirements

Here are the requirements for the High Availability feature:

- One Firebox in each HA pair is the primary Firebox. We recommend that you use the Firebox® with the maximum license features and capacities as the primary HA device.
- The two Fireboxes in an HA configuration must be the same model and must use the same software version. If the software versions are different, you must upgrade the Firebox with the old version to match the other Firebox. The Firebox with the old software must have a license for the upgraded software.
- Each active interface on the primary HA Firebox must connect to the same hub or switch as its matching active interface on the secondary HA Firebox.
- When you connect two Firebox devices in an HA cluster, connect the cable between the highest-number port on each Firebox. If you are configuring two HA connections between the Firebox

devices, use the two highest numbered ports on each Firebox. We recommend that you connect the ports after you configure them.

- HA does not operate correctly if one of the Fireboxes in the HA pair is a VPN endpoint in a VPN tunnel created and managed by the Management Server.
- You cannot put a WatchGuard Management Server behind a gateway Firebox that is part of an HA cluster.

Note

High availability requires an interface or interfaces dedicated specifically for HA synchronization.

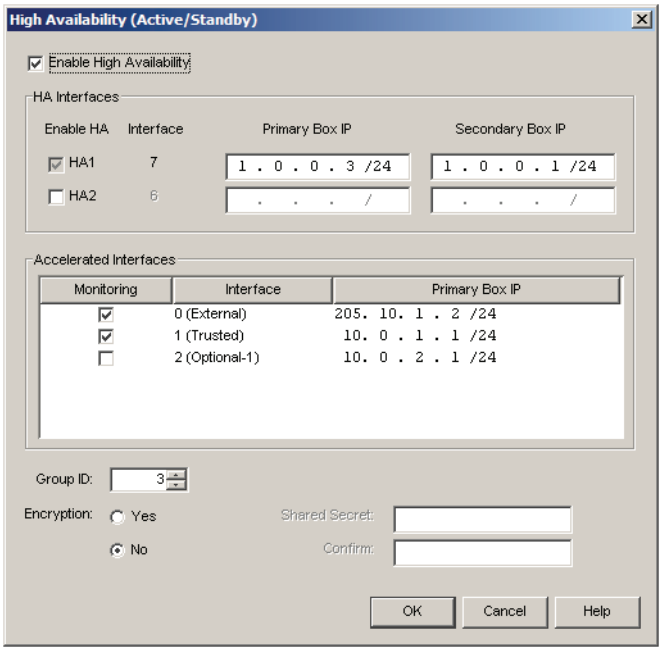
Selecting a Primary High Availability Firebox

When you activate High Availability, each Firebox® in the pair must have a Fireware® feature key enabling the same version of Fireware appliance software. We recommend that you select the Firebox with the most features as the primary Firebox. If you purchase an upgrade for your High Availability pair, you must apply the upgrade to the serial number of the primary Firebox when you activate the upgrade on the LiveSecurity web site. Both Fireboxes in the High Availability pair will use the license features of the primary Firebox.

If you use IPSec VPN tunnels that use a VPN certificate for authentication, the secondary Firebox must get its own IPSec VPN certificate. Only the Management Server certificate is copied from the primary Firebox to the secondary Firebox when a failover occurs.

Configuring HA for Firebox X e-Series Devices

1 From Policy Manager on the primary HA Firebox, select **Network > High Availability**.
The High Availability dialog box appears.



2 Select the **Enable High Availability** check box.

3 Select the **HA1** check box for the interface to enable for High Availability.

4 In the **Primary Box IP** text box, you can change the default IP address if you want. This IP address should be from a reserved or unassigned network. This becomes the permanent IP address for that interface.

5 In the **Secondary Box IP** text box, type an IP address from the same subnet as the interface with High Availability enabled on the active Firebox®.
If you do not change the default primary Firebox IP address, do not change the default secondary box IP address.

6 If you want to use the second HA interface, select the **HA2** check box to enable it.
The HA2 interface is optional.

7 You can select the interfaces you want to monitor for physical link status. The Firebox monitors the selected interfaces and, if the interface is not active, starts an HA failover. Click the check box adjacent to the interface name to enable monitoring. Clear the check box adjacent to the interface name to turn off monitoring of an interface.
It is a good idea to monitor all enabled interfaces.

8 Use the **Group ID** value control to identify this HA group on the network. If you use more than one HA pair on the same network, this number must be different for each pair.

9 Click the **Yes** radio button to encrypt all HA traffic between the Fireboxes. This is usually not necessary, and uses more resources.
or
Click the **No** radio button to not encrypt HA traffic between the Fireboxes.

10 (If you selected the **Yes** radio button) In the **Shared Secret** field, type a shared secret to encrypt HA traffic between the Fireboxes. Type the shared secret again in the **Confirm** field.

11 Save this configuration to the active Firebox.

12 Close Policy Manager.

Configuring the secondary High Availability Firebox

The secondary High Availability Firebox must:

- Be the same model as the primary HA Firebox
- Have a valid feature key

Before you enable the secondary Firebox for HA, you must first use the Web Quick Setup Wizard to install Fireware® and a basic configuration on the Firebox. When the Web Quick Setup Wizard is complete, put the Firebox on your network.

Enabling High Availability

After the primary and secondary HA Fireboxes are configured:

1 Open Firebox System Manager for the Firebox you want to be the secondary HA Firebox.

2 Select **Tools > High Availability > Enable as Secondary**.
The Confirm Enable as Secondary warning box appears.

Confirm Enable As Secondary
The Firebox configuration will be reset to a default state. The Firebox will then be ready to be used as a secondary Firebox in an HA pair.
Are you sure you want to proceed?
Yes
No

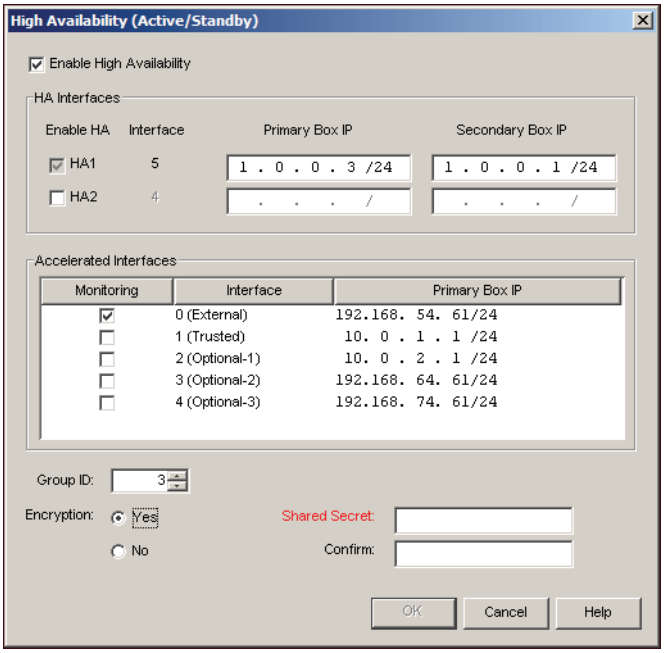
3 Click **Yes** to reset the Firebox to its default state and configure it as the secondary HA Firebox in the HA pair.
You must type the configuration passphrase for the secondary HA Firebox.

4 Use a crossover cable to connect the HA1 interface (eth7) on one Firebox to the HA1 interface on the other Firebox. If HA2 (eth6) is enabled, connect both HA2 interfaces as well.

5 Open Firebox System Manager for the primary HA Firebox and select **Tools > High Availability > Synchronize Configuration**. When prompted, type the configuration passphrase.
You see a message that says High Availability is enabled.

Configuring HA for Firebox X (non e-Series) Devices

1 From Policy Manager, select **Network > High Availability**.
The High Availability dialog box appears.



2 Select the **Enable High Availability** check box.

3 Select the **HA1** check box for the interface to enable for High Availability.

4 In the **Primary Box IP** text box, you can change the default IP address. This IP address should be from a reserved or unassigned network. This becomes the permanent IP address for that interface.

5 In the **Secondary Box IP** text box, type an IP address from the same subnet as the interface with High Availability enabled on the active Firebox®.

6 Select the **HA2** check box to enable the HA2 interface.
The HA2 interface is optional.

7 Use the **Group ID** value control to identify this HA group on the network. If you use more than one HA pair on the same network, this number must be different for each pair.

8 Click the **Yes** radio button to encrypt all HA traffic between the Fireboxes. This is usually not necessary, and uses more resources.
or
Click the **No** radio button to not encrypt HA traffic between the Fireboxes.

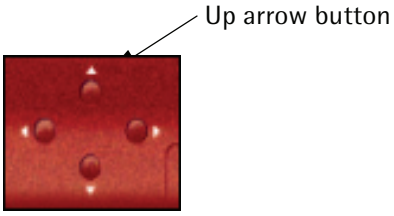
9 (If you selected the **Yes** radio button) In the **Shared Secret** field, type a shared secret to encrypt HA traffic between the Fireboxes. Type the shared secret again in the **Confirm** field.

10 Save this configuration to the active Firebox.

11 Close Policy Manager.

12 Use a crossover cable to connect the HA1 interface (eth5) on one Firebox to the HA1 interface on the other Firebox. If HA2 (eth4) is enabled, connect both HA2 interfaces as well.

13 Put the secondary unit in safe mode. To do this, turn the Firebox off, and then turn it back on while you hold down the up arrow button on the Firebox front panel.



14 Start Firebox System Manager and connect to the primary Firebox.

15 Select **Tools > High Availability > Synchronize Configuration**. When prompted, type the configuration passphrase.
You see a message that says High Availability is enabled.

Manually Controlling High Availability

Although High Availability operations usually occur automatically, you can do some of the functions manually.

Forcing a failover

You can cause a failover to occur. The standby system becomes the active one immediately.

From Firebox® System Manager, select **Tools > High Availability > Force Failover**.

Synchronizing the configuration

You must synchronize the configuration when one Firebox configuration changes while the other is disconnected from the HA peer or turned off.

From Firebox System Manager, select **Tools > High Availability > Synchronize Configuration**.

Restarting the peer

When you connect to an HA configuration, you communicate only to the active Firebox. To restart the peer Firebox, you must send the command from the active Firebox:

From Firebox System Manager, select **Tools > High Availability > Restart Peer**.

Note

When the Firebox is in a high CPU or traffic condition and you use Firebox System Manager to control HA operations, you can get an incorrect “time-out” message. In this case, the operation could have completed, and it is possible the time-out message is not correct.

Backing up an HA configuration

When a Firebox is in a High Availability pair, you can back up the flash image of the Firebox only when it is the active Firebox. This is because the backup image includes the system and policy information, certificates, and licenses that do not exist on the secondary Firebox until failover. To create a backup image (.fxi) of the active Firebox:

1 From Policy Manager, select **File > Backup**.
2 Type the configuration passphrase. Click **OK**.
3 Type and confirm an encryption key. This key is used to encrypt the backup file.
Type a strong encryption key that is easy to remember.
4 Browse or type the location for the backup file. Click **OK**.
The backup file is created.
5 Click **OK** when the backup is complete.

Upgrading Software in an HA Configuration

If you install the software on the active Firebox®, the standby Firebox in the HA configuration does not automatically upgrade. You must upgrade each Firebox. Upgrade the active Firebox first. When it restarts, the standby becomes the active Firebox. You can then upgrade that Firebox. You cannot upgrade the software on a Firebox that is in standby mode.

Using HA with Signature-based Security Services

Gateway AntiVirus and Intrusion Prevention Service (IPS) signature databases do not automatically synchronize between active and standby HA devices.

If the antivirus and IPS features are enabled and an event occurs that causes the standby Firebox® to become active, this device can have a version of the Gateway AntiVirus and IPS signature databases that is not current (especially if it was in standby mode for a long time). Until an update of the database occurs, there is some time when a new virus or IPS attack can bypass the Firebox.

To minimize this problem, keep the automatic signature update intervals for Gateway AntiVirus and Intrusion Prevention Service enabled and short. If possible, force a manual signature update on the new active Firebox immediately after the failover occurs.

Using HA with Proxy Sessions

When High Availability is activated with the default configuration, all outgoing TCP sessions are disconnected when a failover event occurs. Users must manually reestablish all interactive or persistent sessions. This is because proxy session state is not retained between HA peers, and the default configuration has a default TCP-proxy for all sessions. Packet filter sessions are maintained, but the packet filter is not used by default. Consider adding specific packet filter policies to your configuration for telnet, ssh, or any other policy for which you want failover. Note that IPS does not operate with these new policies.

APPENDIX A

Copyright and Licensing

WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:
This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, (1) if the SOFTWARE PRODUCT was bundled with a hardware product, promptly return the SOFTWARE PRODUCT and hardware product, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT and hardware product for a full refund of the price you paid or (2) if the SOFTWARE PRODUCT was sold separately, promptly return any license key for the SOFTWARE PRODUCT, along with proof of payment, to (i) the authorized dealer from whom you obtained the SOFTWARE PRODUCT or (ii) if purchased directly from WATCHGUARD, to WATCHGUARD for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5.United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6.Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7.Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8.Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 050309

WatchGuard Technologies, Inc. Add-on Product/Service Customer Agreement/End-User License Agreement

IMPORTANT: READ CAREFULLY. THIS ADD-ON PRODUCT/SERVICE CUSTOMER AGREEMENT/END-USER LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU THE CUSTOMER ("CUSTOMER"), AND WATCHGUARD TECHNOLOGIES, INC. ("WATCHGUARD"). TO ACTIVATE THE WATCHGUARD ADD-ON PRODUCT/SERVICE DESCRIBED BELOW (THE "ADD-ON PRODUCT/SERVICE"), OR RENEW/UPGRADE YOUR ADD-ON PRODUCT/SERVICE, YOU MUST FIRST READ THIS AGREEMENT AND AGREE TO ACCEPT ITS TERMS BY INDICATING YOUR ACCEPTANCE AS PROMPTED BY THE TEXT ASSOCIATED WITH THE PRESENTATION OF THIS AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, YOUR ACTIVATION/

RENEWAL/UPGRADE REQUEST WILL NOT BE ACCEPTED AND YOU WILL NOT HAVE ACCESS TO THE ADD-ON PRODUCT/SERVICE OR YOUR RENEWAL/UPGRADE REQUEST WILL NOT BE ACCEPTED. IF YOU WISH TO DECLINE ACCEPTANCE, YOU MAY INDICATE THAT YOU DECLINE AS PROMPTED BY THE TEXT ASSOCIATED WITH THE PRESENTATION OF THIS AGREEMENT. IF YOU DO NOT ACCEPT THIS AGREEMENT, YOUR PURCHASE WILL NOT BE COMPLETED OR YOU MAY PROMPTLY RETURN THE LICENSE KEY FOR THE ADD-ON PRODUCT/SERVICE (DEFINED BELOW), ALONG WITH PROOF OF PAYMENT, TO THE AUTHORIZED DEALER or, if purchased directly from WATCHGUARD, to WATCHGUARD, FOR A FULL REFUND OF THE PRICE YOU PAID.

WatchGuard and Customer hereby agree as follows:

1 Definitions. As used herein, the following capitalized terms shall have the following meanings: "Add-on Product/Service" means the software license and renewable subscription service made generally available by WatchGuard to its customers purchasing the equivalent product/service (including level of service, if applicable) as indicated on the License Key, which may include the provision of/access to Software, Threat Signatures, information or other items/services, and which is subject to change by WatchGuard from time to time. "Software" means any WatchGuard software, which includes computer software components (whether installed separately on a computer workstation or on a WatchGuard hardware product or included/pre-installed with a WatchGuard hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent) or the Add-on Product/Service. ''License Key'' means the license key or other written or online documentation provided to Customer evidencing Customer's purchase or renewal/upgrade (as applicable) of the Add-on Product/Service. ''Threat Signatures'' means information used to scan for and identify known cyber-threats that fall into specific classes (e.g., virus signatures or intrusion prevention signatures).

2 Add-on Product/Service. WatchGuard will make the Add-on Product/Service available to Customer during the Term. Customer agrees that (i) an Add-on Product/Service (and all benefits associated with the Add-on Product/Service) may only be used in conjunction with that number of WatchGuard products as expressly provided for in the License Key and that additional Add-on Product/Service licenses/subscriptions must be purchased for additional WatchGuard products that are to receive any benefits of the Add-on Product/Service and (ii) a renewal/upgrade to an Add-on Product/Service (and all benefits associated with the Add-on Product/Service renewal/upgrade) may only be used in conjunction with that number of WatchGuard products as expressly provided for in the renewal/upgrade License Key and that additional renewals/upgrades must be purchased for additional WatchGuard products that are to receive any benefits of the renewal/upgrade.

3 Add-on Product/Service Fees. Customer will pay to WatchGuard the applicable Add-on Product/Service fee and any and all applicable Add-on Product/Service renewal/upgrade fees for Add-on Product/Service renewals/upgrades purchased, each as established by WatchGuard from time to time. The Add-on Product/Service and Add-on Product/Service renewal/upgrade fees are non-refundable to Customer, even in the event of the termination of this Agreement pursuant to Section 6 prior to the expiration of the initial Term, or any renewal of the Term.

4 Term. The term of this Agreement ("Term") shall commence upon acceptance of this Agreement and activation of the Add-on Product/Service or Add-on Product/Service renewal/upgrade by Customer, and shall end upon expiration of the term specified in the applicable License Key, unless renewed in accordance with Section 5 or sooner terminated in accordance with Section 6. The term of the WatchGuard Firebox Software End-User License Agreement applicable to all Software associated with the Add-on Product/Service as described below shall be as stated in such end-user license agreement.

5 Renewal. WatchGuard may establish different renewal options from time to time that will be effective as a renewal pursuant to this Section 5 once payment is made in accordance with such option. Notwithstanding the foregoing, renewals may not be available to Customers with WatchGuard products that have been discontinued or that WatchGuard no longer supports for purposes of the Add-on Product/Service.

6 Termination. Either party may terminate this Agreement if the other party is in material breach and fails to cure such breach within fifteen (15) days of receipt of written notice of such breach, except that WatchGuard may terminate this Agreement immediately upon Customer's failure to pay any applicable fees when due.

7 Software License. Customer expressly agrees that use of all Software associated with the Add-on Product/Service shall be governed solely by the terms and conditions of the WatchGuard Firebox Software End-User License Agreement as a "SOFTWARE PRODUCT"or, if applicable, the WatchGuard software end-user license agreement associated with such Software, and such terms and conditions are incorporated herein by reference.

8 Disclaimer and Release. Warranty Disclaimer. WatchGuard warrants that the Add-on Product/Service will be provided to Customer in accordance with all the requirements of this Agreement. WATCHGUARD MAKES NO OTHER GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE, WITH RESPECT TO THE ADD-ON PRODUCT/SERVICE OR THE ACCURACY, RELIABILITY, OR COMPLETENESS OF ANY THREAT SIGNATURES, INFORMATION OR OTHER ITEM/SERVICE (OR UPDATES THERETO) PROVIDED OR MADE AVAILABLE AS PART OF OR IN CONNECTION WITH THE ADD-ON PRODUCT/SERVICE. WATCHGUARD SHALL NOT BE LIABLE FOR ANY DAMAGES INCURRED AS A RESULT OF ANY USE OF OR RELIANCE UPON THE ADD-ON PRODUCT/SERVICE OR ANY THREAT SIGNATURES, INFORMATION OR OTHER ITEM/SERVICE PROVIDED OR MADE AVAILABLE AS PART OF OR IN CONNECTION WITH THE ADD-ON PRODUCT/SERVICE. THE WARRANTY CONTAINED IN THE FIRST SENTENCE OF THIS PARAGRAPH 8 IS EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO THE ADD-ON PRODUCT/SERVICE OR THE ACCURACY, RELIABILITY, OR COMPLETENESS OF ANY THREAT SIGNATURES, INFORMATION OR OTHER ITEM/SERVICE (OR UPDATES THERETO) PROVIDED OR MADE AVAILABLE AS PART OF OR IN CONNECTION WITH THE ADD-ON PRODUCT/SERVICE (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE CAUSED BY OR CONTRIBUTED TO BY, THE ADD-ON PRODUCT/SERVICE). Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusions may not apply to Customer. This limited warranty gives Customer specific legal rights, and Customer may also have other legal rights, which vary from jurisdiction to jurisdiction.

9 Limitation of Liability. WATCHGUARD'S LIABILITY TO CUSTOMER (WHETHER ARISING IN TORT, CONTRACT OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) UNDER THIS AGREEMENT OR WITH RESPECT TO THE ADD-ON PRODUCT/SERVICE WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY SUBCRIBER FOR THE ADD-ON PRODUCT/SERVICE. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT SHALL WATCHGUARD OR ITS SUPPLIERS BE LIABLE TO CUSTOMER OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OR FAILURE TO PERFORM THE ADD-ON PRODUCT/SERVICE, EVEN IF WATCHGUARD OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. Some jurisdictions do not allow these limitations or exclusions, so they may not apply to Customer.

10 Reservation of Rights. WatchGuard and its licensors hereby reserve ownership of and all rights in the Threat Signatures, information and other items/services provided or made available as part of or in connection with the Add-on Product/Service and all copyrights, trademarks and other proprietary rights associated with such Threat Signatures, information and other items/services. Except as provided for in this Agreement or as expressly authorized by WatchGuard in writing (including by publishing the terms and

conditions of use by WatchGuard of any Threat Signatures subject to "open source" licensing), you may not reproduce, republish, post, transmit or distribute the Threat Signatures, information or other items/services provided as part of the Add-on Product/Service.

11 Entire Agreement. This Agreement, together with the WatchGuard License Key, the WatchGuard Firebox Software End-User License Agreement, any software end-user license agreements accompanying the Software licensed to Customer, and any agreement between Customer and WatchGuard explicitly stating that the terms of such agreement control over the terms of any of the agreements listed in this sentence in the case of any conflict or inconsistency, constitutes the entire Agreement between WatchGuard and Customer and supersedes any and all prior or contemporaneous statements, representations and agreements, written or oral, with regard to the Add-on Product/Service. If the Customer has purchased the right to utilize the Add-on Product/Service on additional WatchGuard products, this Agreement will therefore supersede all prior customer agreements/end-user license agreements applicable to the same Add-on Product/Service and the terms of this Agreement shall govern all uses of this Add-on Product/Service by Customer. This Agreement may be amended or modified only by a written instrument executed by both parties or by Customer accepting a subsequent customer agreement for this Add-on Product/Service provided by WatchGuard.

THIS AGREEMENT SHALL BE GOVERNED BY AND CONSTRUED UNDER THE LAWS OF THE STATE OF WASHINGTON, WITHOUT REFERENCE TO ITS CONFLICT OF LAW PRINCIPLES. The parties consent to the personal and exclusive jurisdiction of courts located in Washington, King County. Customer may not assign this Agreement (by operation of law or otherwise) without the prior written consent of WatchGuard. This Agreement will be binding upon and will inure to the benefit of the parties' permitted successors and/or assignees. Waiver by either party of a breach or any provision of this Agreement or the failure by either party to exercise any right hereunder shall not operate or be construed as a waiver of any subsequent breach of that right or as a waiver of any other right. Neither party shall be considered to be in breach of this Agreement on account of any delay or failure to perform any obligation hereunder (other than a delay or failure in the payment of money) as a result of any cause or condition beyond such party's reasonable control.

IF YOU AGREE TO THE TERMS OF THIS AGREEMENT, INDICATE YOUR ACCEPTANCE AS PROMPTED BY THE TEXT ASSOCIATED WITH THE PRESENTATION OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, INDICATE THAT YOU DECLINE AS PROMPTED BY THE TEXT ASSOCIATED WITH THE PRESENTATION OF THIS AGREEMENT. BY ACCEPTING THIS AGREEMENT, YOU REPRESENT AND WARRANT THAT: (A) THE INDIVIDUAL INDICATING THEIR ACCEPTANCE TO THIS AGREEMENT IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON CUSTOMER'S BEHALF AND TO BIND CUSTOMER TO THE TERMS OF THIS AGREEMENT; (B) CUSTOMER HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF CUSTOMER'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH CUSTOMER IS A PARTY.

Version: 050309

Copyright and Trademarks

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, Windows® 2000, Windows® 2003, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All rights reserved.
Jcchart copyright® 1999 by KL Group Inc. All rights reserved.
WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Patents

U.S. Patent Nos. 6,493,752; 6,597,661; 6,618,755; D473,879. Other Patents Pending.

Licenses

Some components of the WatchGuard System Manager software distribute with source code covered under one or more third party or open source licenses. We include below the full text of the licenses as required by the terms of each license. To get the source code covered under these licenses, please contact WatchGuard Technical Support at:

- 877.232.3531 in the United States and Canada
- +1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

SSL Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

OpenSSL License

© 1998-2003 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,

DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Original SSLeay License

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-2003 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes' SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).''
4. The names ''mod_ssl'' must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called ''mod_ssl'' nor may ''mod_ssl'' appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: ''This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).''
THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache Software License, Version 2.0, January 2004

Some components of the WatchGuard System Manager software are distributed with a version of the Apache web server and other source code under the Apache software license.

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this

License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

PCRE License

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. The PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR

ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU Lesser General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU Lesser General Public License (LGPL).

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different

from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is

true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

GNU General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU General Public License (GPL).

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights,

from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,

INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
END OF TERMS AND CONDITIONS

Sleepycat License

Some components of the WatchGuard System Manager software are distributed with a version of the BerkeleyDB covered under the Sleepycat software license.

Copyright (c) 1990-2004
Sleepycat Software. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs.
THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 1990, 1993, 1994, 1995
The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1996

The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sourcefire License

In addition to the copyright and license information found earlier in this Appendix, signature updates provided as part of the Gateway AV/IPS Subscription are subject to this license agreement:

SOURCEFIRE,INC.

VERSION 1.1.1

THE VRT CERTIFIED RULES ARE MADE AVAILABLE TO YOU BY SOURCEFIRE, INC. ("SOURCEFIRE") UNDER THE TERMS OF THIS VRT CERTIFIED RULES LICENSE AGREEMENT (THE "AGREEMENT"). BY CLICKING THE "ACCEPT" BUTTON BELOW, OR BY INSTALLING OR USING THE VRT CERTIFIED RULES, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT CLICK THE "ACCEPT" BUTTON, AND DO NOT INSTALL OR USE ANY PART OF THE VRT CERTIFIED RULES.

1. Definitions

1.1. "Commercial Purpose" means the use, reproduction or distribution of (i) the VRT Certified Rules or any Modification, or any portion of the foregoing, (ii) a Compilation that includes, in whole or in part, the VRT Certified Rules or any Modification that in either case is intended to result in a direct or indirect pecuniary gain or any other consideration or economic benefit to any person or entity involved in such use, reproduction or distribution. Examples of a Commercial Purpose, include without limitation, (v) integrating the VRT Certified Rules with other software or hardware for sale, (w) licensing the VRT Certified Rules for a fee, (x) using the VRT Certified Rules to provide a service to a third party, (y) selling the VRT Certified Rules, or (z) distributing the VRT Certified Rules for use with other products or other services.

1.2. "Compilation" means a work which combines the VRT Certified Rules or any Modification or portions thereof with any services, programs, code or other products not governed by the terms of this Agreement.
1.3. "Improvements" shall mean a Modification to a VRT Certified Rule (or to a modified VRT Certified Rule) that corrects a bug, defect, or error in such rule without affecting the overall functionality of such VRT Certified Rule (or Modification thereof).
1.4. "Modifications" means any alteration, addition to or deletion from the substance or structure of the VRT Certified Rules or any Modifications of such, including, without limitation, (a) any addition to or deletion from the contents of a file containing Original Code or previous Modifications of either; (b) any derivative of the VRT Certified Rule or of any Modification; or (c) any new file that contains any part of the VRT Certified Rule or Modifications.
1.5. "Permitted Use" shall have the meaning given such term in Section 2.1.
1.6. "Restricted Activities" shall have the meaning given such term in Section 2.1.
1.7. "Snort® Registered User" shall mean an individual who has registered or subscribed on www.snort.org to use the VRT Certified Rules.
1.8. "VRT Certified Rules" means those Snort® rules (in text form, source code form, object code form and all documentation related thereto) that have been created, developed, tested and officially approved by Sourcefire. These rules are designated with SIDs of 3465 - 1,000,000, except as otherwise noted in the license file.
1.9. "You" (or "your") means an individual exercising rights under this Agreement issued under Section 7. For legal entities, "you" includes any entity which controls, is controlled by, or is under common control with you or any such entity you are acting on behalf of. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than forty percent (40%) of the outstanding shares or beneficial ownership of such entity.
2. Sourcefire License Grant.
2.1. Grant of License; Permitted Use. Subject to the terms and conditions of this Agreement, Sourcefire hereby grants you a world-wide, non-exclusive license to do any of the following with respect to the VRT Certified Rules: (a) use and deploy the VRT Certified Rules on management consoles and sensors that you manage (over which you have administrative control); (b) use and deploy the VRT Certified Rules on behalf of your employer on its internal management consoles and sensors (e.g., where a valid employer-employee relationship exists between you and a legal entity); (c) modify the VRT Certified Rules and use those Modifications consistent with paragraphs (a) and (b) above; (d) distribute those VRT Certified Rules and any Modifications generally available to Snort® Registered Users on a limited basis to other Snort® Registered Users; (e) distribute any Improvement generally available to Snort® Registered Users on mailing lists commonly used by the Snort® user community as a whole; (f) reproduce the VRT Certified Rules as strictly necessary in exercising your rights under this Section 2.1; and (g) Make the VRT Certified Rules (or any Modification) available to your or your employer's consultants, agents and subcontractors for the limited purpose of exercising your rights under this Section 2.1 provided that such use is in compliance with this Agreement. Paragraphs (a) through (g) are collectively referred to as the "Permitted Uses". All rights not granted under this Agreement are reserved by Sourcefire.
2.2. Limitations on License; Restricted Activities. You recognize and agree that the VRT Certified Rules are the property of Sourcefire, contain valuable assets and proprietary information and property of Sourcefire, and are provided to you under the terms and conditions of this Agreement. Notwithstanding anything to the contrary in this Agreement, You agree that you shall NOT do any of the following without Sourcefire's prior written consent: (a) use, deploy, perform, modify, license, display, reproduce or distribute the VRT Certified Rules or Modifications (even if merged with other materials as a Compilation) other than as allowed under a Permitted Use; (b) sell, license, transfer, rent, loan, use, modify, reproduce or disclose the VRT Certified Rules or any Modifications thereto (in whole or in part and whether done independently or as part of a Compilation) for a Commercial Purpose; (c) post or make generally available any VRT Certified Rule (in whole or in part or any Modifications thereto) to individuals or a group of individuals who have not agreed to the terms and conditions of this Agreement, provided, however, that nothing in this Section 2.2(c) shall preclude the Permitted Use in Section 2.1(e); (d) share any user authentication information and/or password provided to you by Sourcefire with any third party to allow such party access your snort.org account or to

otherwise access the VRT Certified Rules; (e) alter or remove any copyright notice or proprietary legend contained in or on the VRT Certified Rules. Paragraphs (a) though (e) of this Section 2.2 are collectively referred to as the "Restricted Activities").

2.3. Reproduction Obligations. You agree that any embodiment of the VRT Certified Rules permitted under this Agreement will contain the notices set forth in Exhibit A. In addition, to the extent you make any copies of or distribute the VRT Certified Rules or any Modifications under this Agreement, you agree to ensure that any and all such copies of shall contain: (a) a copy of an appropriate copyright notice and all other applicable proprietary legends; (b) a disclaimer of any warranty consistent with this Agreement; and (c) any and all notices referencing this Agreement and absence of warranties.

3. Modifications; Derivative Works.

In the event you create a Modification, the use, reproduction and distribution of such Modifications shall be governed by the terms and conditions of this Agreement. Additionally, you hereby grant Sourcefire and any other licensee of the VRT Certified Rules an irrevocable, perpetual, fully paid-up, world-wide, royalty-free, non-exclusive license to use, reproduce, modify, display, perform and distribute such Modifications (and the source code thereto), provided, however, that you and any recipient of such Modifications must include: (a) the original copyright notice and all other applicable proprietary legends; (b) the original warranty disclaimer; (c) the original notices referencing this Agreement and absence of warranties; and (d) a prominent notice stating that you changed the VRT Certified Rulese (or any Modification thereto) and the date of any change.

4. Distribution Obligations.

4.1. General. The source code version of the VRT Certified Rules (or any Modification thereof) may be distributed only under the terms of this Agreement, and you must include a copy of this Agreement with every copy of the VRT Certified Rules you distribute.

4.2. Required Notices. You must duplicate the notice in Exhibit A in each file of the source code. If it is not possible to put such notice in a particular source code file due to its structure, then you must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If you created one or more Modification(s) you may add your name as a contributor to the notice described in Exhibit A. You must also duplicate this Agreement in any documentation for the source code where you describe recipients' rights or ownership rights relating to the VRT Certified Rules. To the extent you offer additional warranty, support, indemnity or liability obligations, you may do so only on your own behalf, and not on behalf of Sourcefire. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by you alone, and you hereby agree to indemnify and hold Sourcefire harmless for any liability incurred by Sourcefire as a result of any warranty, support, indemnity or liability terms you offer.

5. Inability to Comply Due to Statute or Regulation.

If it is impossible for you to comply with any of the terms of this Agreement with respect to some or all of the Original Code due to statute, judicial order, or regulation then you must: (a) comply with the terms of this Agreement to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

6. Application of this Agreement.

This Agreement also applies to code to which Sourcefire has attached the notice in Exhibit A and to related Modifications created in Section 3.

7. Versions of the Agreement.

7.1. New Versions. Sourcefire may publish revised and/or new versions of the Agreement from time to time. Each version will be given a distinguishing version number.

7.2. Effect of New Versions. Once VRT Certified Rules has been published under a particular version of the Agreement, you may always continue to use it under the terms of that version. You may also choose to use such VRT Certified Rules under the terms of any subsequent version of the Agreement published by Sourcefire. No one other than Sourcefire has the right to modify the terms applicable to Original Code.

8. DISCLAIMER OF WARRANTY.

THE VRT CERTIFIED RULES AND MODIFICATIONS ARE PROVIDED UNDER THIS AGREEMENT ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE VRT CERTIFIED RULES OR THE MODIFICATIONS ARE FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE VRT CERTIFIED RULES AND MODIFICATIONS IS WITH YOU. SHOULD ANY VRT CERTIFIED RULES OR MODIFICATIONS PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT SOURCEFIRE) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT. NO USE OF ANY VRT CERTIFIED RULE OR ANY MODIFICATION IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

9. Termination.

9.1. This Agreement and the rights granted hereunder will terminate automatically if you fail to comply with any or all of the terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the VRT Certified Rules which are properly granted shall survive any termination of this Agreement. Provisions which, by their nature, must remain in effect beyond the termination of this Agreement shall survive.

10. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU OR SOURCEFIRE BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, SECURITY BREACHES OR FAILURES, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATIONS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

11. License Compliance.

You may be requested by Sourcefire to provide a certificate, signed by your authorized representative, that you are using the VRT Certified Rules consistent with a Permitted Use. In the event your use of the VRT Certified Rules is not in compliance with a Permitted Use, or if you otherwise violate the terms of this Agreement, Sourcefire may, since remedies at law may be inadequate, in addition to its other remedies: (a) demand return of the VRT Certified Rules; (b) forbid and enjoin your further use of the VRT Certified Rules; (c) assess you a use fee appropriate to your actual use of the VRT Certified Rules.

12. United States Government Users.

If the VRT Certified Rules or Modifications are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in the VRT Certified Rules and Modifications shall be subject to Sourcefire's standard commercial terms and only as set forth in this Agreement; and only with "Limited Rights" and "Restricted Rights" as defined the federal regulations if the commercial terms are deemed not to apply.

13. Miscellaneous.

This Agreement represents the complete agreement concerning subject matter hereof. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be governed by Maryland law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. Any litigation relating to this Agreement shall be subject to the jurisdiction of the state and Federal Courts serving Greenbelt, Maryland, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. You hereby submit to jurisdiction and venue in such courts. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not

apply to this Agreement. Headings and section references are used for reference only and shall not be used to define, limit or describe such section.

EXHIBIT A - VRT Certified Rules License Agreement

The contents of this file are subject to the VRT Certified Rules License Agreement 1.1 (the "Agreement"). You may not use this file except in compliance with the Agreement. You may obtain a copy of the Agreement here. Software distributed under the Agreement is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the Agreement for the specific language governing rights and limitations under the Agreement. The developer of the VRT Certified Rules is Sourcefire, Inc., a Delaware Corporation.

Expat-MIT HTML Parser Toolkit License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:
The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Curl Software MIT-X License

COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>.
All rights reserved.
Permission to use, copy, modify, and distribute this software for any purpose
with or without fee is hereby granted, provided that the above copyright
notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN
NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE
OR OTHER DEALINGS IN THE SOFTWARE.
Except as contained in this notice, the name of a copyright holder shall not
be used in advertising or otherwise to promote the sale, use or other dealings
in this Software without prior written authorization of the copyright holder.

Note

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

APPENDIX B

WatchGuard File Locations

This appendix gives the location where common data files are kept by the WatchGuard® System Manager software. Since it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must know the correct location of these files based on the configuration of Windows on your computer.

It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply.

If you are using an OS version that is not English, you must translate directory names (such as "Documents and Settings" or "Program Files") to match the OS language you use.

File Type	Location
User-created data	My Documents\My WatchGuard (User created data includes files such as Firebox configuration files, license files, and certificates. In many cases, the WSM software creates subfolders in the My WatchGuard folder to keep these files.)
User-created data (shared)	C:\Documents and Settings\All Users\Shared WatchGuard
Firebox® configuration files	My Documents\My WatchGuard\configs
Firebox log files	C:\Documents and Settings\WatchGuard\logs
Report files	C:\Documents and Settings\WatchGuard\reports
Certificates	My Documents\My WatchGuard
WatchGuard® applications	C:\Program Files\WatchGuard\wsm8
Shared application libraries	C:\Program Files\Common Files\WatchGuard\wsm8
Management Server data	C:\Documents and Settings\WatchGuard\wmserver
Certificate Authority data	C:\Documents and Settings\WatchGuard\wmserver\wgca
WebBlocker Server data	C:\Documents and Settings\WatchGuard\wbserver
Future product upgrade images	C:\Program Files\Common Files\WatchGuard\resources

File Type	Location
Help files (Fireware®)	C:\Program Files\WatchGuard\wsm8\help
Help files (WFS)	C:\Program Files\WatchGuard\wsm8\wfs\help

Default File Locations

These tables gives the default location where the WatchGuard® software applications and servers look for their data files or for data files created by users (such as Firebox® configuration files). In some cases, the default location changes based on where the software application opened a file of a similar type. In these cases, the software application remembers the last place the file was read/written and looks in that location first.

Since it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must determine the exact location of these files based on the configuration of Windows on your computer.

It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply.

If you are using an OS version that is not English, you must translate directory names (such as "Documents and Settings" or "Program Files") to match the OS language you use.

Policy Manager for Fireware Appliance Software

Operation	File Type	Default Location
Read/Write	Firebox backups	C:\Documents and Settings\All Users\Shared WatchGuard\backups
Read	Product upgrade images	C:\Program Files\Common Files\WatchGuard\Resources\Fireware
Read	Blocked Sites	My Documents\My WatchGuard
Read	Blocked Sites exceptions	My Documents\My WatchGuard
Read/Write	Firebox configuration files	My Documents\My WatchGuard\configs
Read/Write	Firebox license files	My Documents\My WatchGuard\configs
Read	Initial license import	My Documents\My WatchGuard
Write	MUVPN .wgx File	C:\Documents and Settings\All Users\Shared WatchGuard\ muvpn

Policy Manager for WFS Appliance Software

Operation	File Type	Default Location
Read	Logging Notification	Current working directory
Read	Spam rules import	Current working directory
Write	Saved backups	C:\Documents and Settings\All Users\Shared WatchGuard\ backups
Write	MUVPN SPDs (.wgx)	C:\Documents and Settings\All Users\Shared WatchGuard\ muvpn
Read	Blocked Sites imports	Current working directory

Flash Disk Management for WFS Appliance Software

Operation	File Type	Default Location
Read/Write	Backup image	C:\Documents and Settings\All Users\Shared WatchGuard\ backups

Historical Reports

Operation	File Type	Default Location
Read/Write	Report definitions	C:\Documents and Settings\WatchGuard\report-defs
Read/Write	Reporting graphics	C:\Program Files\WatchGuard\wsm8\reports\graphics\ <report .jpg/.gif files>

APPENDIX C

Types of Policies

This chapter gives a list of the pre-defined policies included with Fireware® appliance software, their protocols, and their ports. It also gives special information about circumstances that could have an effect on the security of some policies.

In this chapter, policies are divided into two groups—policies that are controlled by a packet filter and policies that are controlled by a proxy.

Packet Filter Policies

Packet filter policies examine the source and destination headers of each packet. Packets are allowed or denied based on if the headers appear to come from and go to trusted addresses.

Any

Use an Any policy only to allow all traffic between two specified trusted IP or network addresses. An Any policy opens a "hole" through the Firebox®, and allows all traffic to flow freely between specified hosts. We recommend that the Any policy be used only for traffic through a VPN.

The Any policy is different from other policies. For example, if you allow FTP only to a specified host, all other FTP sessions to other hosts are denied by that policy (unless you have also configured other FTP policies). The Any policy does not deny like other policies.

You also cannot use an Any policy unless specified IP addresses, network addresses, host aliases, group names, or user names are used in the **From** or **To** lists. If not, the Any policy does not operate.

Characteristics

- Internet Protocol(s): Any
- Port Number(s): Any port

AOL

The America Online proprietary protocol allows access to AOL through a TCP/IP network. The AOL client must be specially configured to use TCP/IP and not a modem.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 5190

archie

archie is a search protocol used to find files on FTP servers. We recommend that you use the available web interfaces to archie. A current list of archie servers is available through anonymous FTP from:

ftp://microlib.cc.utexas.edu/microlib/mac/info/archie-servers.txt

External hosts can be spoofed. The Firebox cannot make sure that these packets were sent from the correct location. You can configure your Firebox to add the source IP address to the Blocked Sites list when an incoming archie connection is denied. You can use all of the usual log options with archie.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 1525

auth

The Authentication Server protocol (AUTH) has a new name. It is now called the Identification Protocol (IDENT). Refer to IDENT for more information about this policy.

BGP

Border Gateway Protocol (BGP) is the routing protocol used across most of the Internet. It is a highly configurable protocol that can add redundancy to links to and from the Internet for LANs. We recommend that you use this service only if you have enabled and configured BGP in the dynamic routing processes in the Fireware® configuration.

Characteristics

- Internet Protocol(s): TCP or UDP
- Port Number(s): 179

Citrix

Citrix, or Independent Computing Architecture (ICA), is an application protocol used by Citrix software applications such as Winframe and Metaframe Presentation Server (MPS). Winframe gives access to a Windows computer from different types of clients that use TCP port 1494. Citrix MPS 3.0 uses ICA with Session Reliability over TCP port 2598. If you use Citrix MPS, you must add a custom policy for TCP port 2598. If you add the Citrix policy, you could put your network security at risk because it allows remote access to computers through the firewall without authentication. The threat to a Winframe or MPS

server includes denial-of-service attacks. We recommend that you use VPN options to give more security for ICA connections. You can use all of the usual log options with WinFrame.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1494

For more information on how to add the Citrix ICA policy, refer to the Advanced FAQs in the Knowledge Base. Go to www.watchguard.com/support and log in to the LiveSecurity Service.

Clarent-gateway

Clarent Corporation supplies IP telephone technology to mainstream carriers and service providers. Clarent products allow voice-over-IP between Clarent gateways across the Internet. This policy gives support to the Clarent v3.0 product and later.

Clarent products use two sets of ports, one for gateway-to-gateway communications (UDP ports 4040, 4045, and 5010) and one for gateway-to-command center communications (UDP ports 5001 and 5002). Use the Clarent-command policy for the gateway-to-command center communications.

Allow incoming connections only from specified external gateways to your gateway or command center.

Clarent also gives support for the use of PCAnywhere for management. Refer to the PCAnywhere policy notes for more information.

The Clarent-gateway policy could put network security at risk because it allows traffic inside the firewall based only on network address. This is not a trusted method of authentication. In addition, your Clarent server could receive denial-of-service attacks in this configuration. Where possible, we recommend that you use VPN options to give more security for Clarent-gateway connections.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 4040, 4045, 5010

Clarent-command

Clarent Corporation supplies IP telephone technology to mainstream carriers and service providers. Clarent products allow voice-over-IP between Clarent gateways across the Internet. This policy gives support to the Clarent v3.0 product and later.

Clarent products use two sets of ports, one for gateway-to-gateway communications (UDP ports 4040, 4045, and 5010) and one for gateway-to-command center communications (UDP ports 5001 and 5002). Use the Clarent-command policy for the gateway-to-command center communications.

Allow incoming connections only from specified external gateways to your gateway or command center.

Clarent also gives support for the use of PCAnywhere for management. Refer to the PCAnywhere policy notes for more information.

The Clarent-command policy could put network security at risk because it allows traffic inside the firewall based only on network address. This is not a trusted method of authentication. In addition, your Clarent server could receive denial-of-service attacks in this configuration. Where possible, we recommend that you use VPN options to give more security for Clarent-command connections.

Characteristics:

- Internet Protocol(s): UDP
- Port Numbers(s): 5001, 5002

CU-SeeMe

CU-SeeMe is a software application used to do video conferencing through the Internet. For CU-SeeMe to operate through the Firebox, you must make sure that you are not on a network that uses outgoing dynamic NAT. Configure the CU-SeeMe policy for incoming and outgoing access.

The CU-SeeMe protocol makes you configure this policy for incoming and outgoing. The CU-SeeMe policy uses the correct ports to allow the use of CU-SeeMe versions 2.X and 3.X. CU-SeeMe Version 2.X operates on UDP port 7648. Version 3.X operates on UDP port 7648, UDP port 24032 (for H.323 conferences), and TCP port 7648 (video conference directories).

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Numbers(s): UDP 7648, UDP 24032, TCP 7648

DHCP-Server or DHCP-Client

Dynamic Host Configuration Protocol (DHCP) gives a way to allocate dynamic IP addresses to devices on a network.

Characteristics

- Internet Protocol(2): TCP
- DHCP-Server Port Number(s): 68
- DHCP-Client Port Number(s): 67

DNS

Domain Name Service (DNS) matches host names to IP addresses. A DNS policy is enabled in the default configuration. The DNS policy allows UDP DNS traffic, as well as TCP zone transfers to occur as specified. All of the usual log options can be used with DNS.

Characteristics

- Internet Protocol(s): Multi: TCP (for server-server zone transfers) and UDP (for client-server lookups)
- Port Number(s): TCP 53 and UDP 53

Entrust

The Entrust Authority Public Key distribution application protocol passes public keys to a trusted third-party organization for verification.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 709, 710

finger

finger is an application protocol used to get information about users on a given host. It is easy for a hacker to use this information against you. We do not recommend that you put finger servers on the trusted interface.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 79

FTP

File Transfer Protocol (FTP) is used to move files across the Internet. An FTP packet filter will not apply the FTP proxy rule set to any traffic. To proxy FTP traffic, use the FTP proxy policy. We recommend that incoming FTP be allowed only to public FTP servers located behind the Firebox.

External hosts can be spoofed. WatchGuard cannot verify that these packets were actually sent from the correct location. You can configure the Firebox to add the source IP address to the Blocked Sites list whenever an incoming FTP connection is denied. The packet filter and proxy policy included in WatchGuard Policy Manager handles the data channel for active and passive FTP sessions. All of the usual log options can be used with FTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): FTP uses two ports: TCP 20 for control connections and TCP 21 for data transfer. TCP 21 can be an incoming or outgoing connection depending on how the client is configured. If it is incoming, 21 is the source port, and the destination port is random.

Gopher

Gopher is a data-retrieval protocol developed at the University of Minnesota. Gopher is not frequently used, as most users use HTML.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 70, but servers can be configured to use other ports

GRE

Generic Routing Encapsulation Protocol (GRE) is used together with Point-to-Point Tunneling Protocol (PPTP) to create virtual private networks (VPNs) between clients or between clients and servers.

Characteristics

- Internet Protocol(s): GRE
- Protocol Number(s): 47

HTTP

A HTTP packet filter will not apply the HTTP proxy rule set to any traffic. To proxy HTTP traffic, use the HTTP proxy policy. We recommend that incoming HTTP be allowed only to public HTTP servers located behind the Firebox.

External hosts can be spoofed. WatchGuard cannot verify that these packets were actually sent from the correct location. You can configure the Firebox to add the source IP address to the Blocked Sites list whenever an incoming HTTP connection is denied. All of the usual log options can be used with HTTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 80

HTTPS

HTTPS is a secure and encrypted version of the HTTP protocol. The client and the web server set up an encrypted session on TCP port 443. Because this session is encrypted, the proxy cannot examine packet contents using a proxy. This policy uses a packet filter to examine the connection.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 443

HBCI

The Home Banking Computer Interface (HBCI) is a standard created for bank customers and manufacturers of banking products.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 3000

IDENT

The Identification Protocol (IDENT) is a protocol used to match TCP connections to a user name. It is used most frequently by large public SMTP and FTP servers. It is used for logs, but you cannot trust the information it gives, as attackers can change their servers to have them send back incorrect information. IDENT uses “fake” information to hide internal user information.

When you use SMTP with incoming static NAT, you must add IDENT to your Policy Manager. Configure IDENT to allow traffic to the Firebox. This enables mail messages to flow from behind the Firebox to the many SMTP servers on the Internet that use IDENT to identify other mail servers’ identities, and allows these servers to return messages through the Firebox to their senders.

If you are not using dynamic NAT, allow IDENT to the IP address of your e-mail server.

We recommend that IDENT policies be allowed to and from the Firebox, but know that hackers can use IDENT to collect user names.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 113

IGMP

The Internet Group Management Protocol (IGMP) is the standard for IP multicasting on the Internet. It is used to control host memberships in multicast groups on a single network.

Characteristics

- Internet Protocol(s): IGMP

IKE

The Internet Key Exchange Protocol is a standard protocol for key management.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 4500 and 500. UDP 4500 is used only for NAT traversal.

IMAP

Internet Mail Access Protocol (IMAP) is an application layer protocol for getting e-mail or bulletin board messages on a remote e-mail server as if the messages were local. You can get access to e-mail stored on an IMAP server from many locations (such as home, work, or laptop) without moving messages.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 143

IPSec

Internet Protocol Security (IPSec) is a framework for a set of protocols for security at the network or packet layer of network communications. It is a VPN tunneling protocol with encryption.

Characteristics

- Internet Protocol(s): UDP, encapsulated security payload (ESP), and authentication header (AH)
- Port Number(s): UDP 500 and UDP 4500

IRC

Internet Relay Chat (IRC) is a system for Internet chatting. To use IRC you must have an IRC client and Internet access. The IRC client is a software application on your computer that sends and receives messages to and from an IRC server. The IRC server makes sure that all messages are sent to all users in the chat session.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 6667

Intel Video Phone

Intel Video Phone is a real-time multimedia application based on H.323. H.323 is an international standard for conferencing over TCP/IP networks. This policy does not filter for dangerous content. It does not support QoS or rsvp protocol, and it does not support NAT.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1720, 522

Kerberos v 4 and Kerberos v 5

The Kerberos network authentication protocol is an authentication system developed by the Massachusetts Institute of Technology (MIT). Kerberos enables two computers to exchange private information across an open network using authentication for security.

Characteristics

- Internet Protocol(s): TCP and UDP
- Kerberos v 4 Port Numbers(s): UDP 750
- Kerberos v 5 Port Number(s): TCP 88 and UDP 88

L2TP

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate virtual private networks.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 1701

LDAP

Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for using online directory services. The protocol operates with Internet transport protocols, such as TCP. You can use LDAP to get access to stand-alone directory servers or X.500 directories.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 389

LDAP-SSL

Lightweight Directory Access Protocol over TLS/SSL (LDAP-SSL) is used with Windows 2000 to give more security when you access Active Directory.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 636

Lotus Notes

Lotus Notes is a client/server platform for conferencing, databases, e-mail. It is also used to create and use documents. This policy enables the proprietary Lotus Notes protocol. Because the protocol uses encapsulation and tunneling, and gives access to internal data, we do not recommend the Lotus Notes policy for addresses out of the trusted network.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1352, UDP 1352

MSSQL-Monitor

Microsoft SQL Monitor is used to monitor Microsoft SQL databases.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1434, UDP 1434

MSSQL-Server

Microsoft SQL Server is usually used to make a remote connection to a Microsoft SQL database.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1433, UDP 1433

MS Win Media

Microsoft Windows Media Server is a proprietary protocol developed by Microsoft to supply unicast streams. It enables bidirectional connections that enable users to go forward, go back, or pause the playback of unicast streams.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1755, 80

NetMeeting

NetMeeting is a product developed by Microsoft Corporation that enables groups to teleconference across the Internet. It is included with Microsoft's Internet Explorer web browser. This policy is based on the H.323 protocol and does not filter for dangerous content. It does not support QoS or rsvp protocol, and it does not support NAT.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1720, 389

NFS

The Network File System (NFS) protocol is a client server software application created by Sun Microsystems to allow all network users to get access to shared files kept on computers of different types.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 2049, UDP 2049

NNTP

Network News Transfer Protocol (NNTP) is used to transmit Usenet news articles.

The best procedure to use NNTP is to set internal hosts to internal news servers and external hosts to news feeds. In most conditions NNTP must be enabled in two directions. If you operate a public newsfeed, you must allow NNTP connections from all external hosts. WatchGuard cannot make sure that these packets were sent from the correct location.

You can configure the Firebox to add the source IP address to the Blocked Sites list when an incoming NNTP connection is denied. All of the usual log options can be used with NNTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 119

NTP

Network Time Protocol (NTP) is a protocol built on TCP/IP that controls local timekeeping. It synchronizes computer clocks with other clocks located on the Internet.

Characteristics

- Internet Protocol(s): UDP and TCP

- Port Number(s): TCP 123 and UDP 123

OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for IP networks based on the link-state algorithm. OSPF is quickly replacing the use of RIP on the Internet because it gives smaller, more frequent updates to routing tables and makes networks more stable.

Characteristics

- Internet Protocol(s): OSPF
- Protocol Number(s): 89

pcAnywhere

pcAnywhere is a software application used to get remote access to Windows computers. To enable this protocol, add the PCAnywhere policy. Then, allow access from the hosts on the Internet that must get access to internal pcAnywhere servers, and to the internal pcAnywhere servers.

pcAnywhere is not a very secure policy and can put network security at risk, because it allows traffic through the firewall without authentication. Also, your pcAnywhere server can receive denial-of-service attacks. We recommend that you use VPN options to give more security.

Characteristics

- Internet Protocol(s): UDP and TCP
- Port Number(s): UDP 22, UDP 5632, TCP 5631, TCP 65301

ping

You can use ping to confirm if a host can be found and is operating on the network. To find DOS-based or Windows-based traceroute packets, configure a ping policy.

Outgoing ping is a good tool for troubleshooting. We do not recommend you enable ping connections incoming to your trusted network.

Characteristics

- Internet Protocol(s): ICMP
- Protocol Number(s): 1

POP2 and POP3

POP2 and POP3 (Post Office Protocol) are e-mail transport protocols, usually used to get a user's e-mail from a POP server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 109 (POP2), and 110 (POP3)

PPTP

PPTP is a VPN tunnel protocol with encryption. It uses one TCP port (for negotiation and authentication of a VPN connection) and one IP protocol (for data transfer) to connect the two peers in a VPN. Configure the PPTP policy to allow access from Internet hosts to an internal network PPTP server. PPTP cannot get access to hosts' static NAT because NAT cannot forward IP protocols. Because this policy enables a tunnel to the PPTP server and the Firebox cannot examine packets in the tunnel, use of this policy must be controlled. Be sure to use the most current version of PPTP.

Characteristics

- Internet Protocol(s): TCP
- PPTP Negotiation Port Number(s): 1723

RADIUS and RADIUS-RFC

The Remote Authentication Dial-In User Service (RADIUS) supplies remote users with secure access to corporate networks. RADIUS is a client-server system that keeps authentication information for users, remote access servers, and VPN gateways in a central user database that is available to all servers. Authentication for the network occurs from one location. RADIUS uses an authentication key that identifies an authentication request to the RADIUS client.

In RFC 2865, the server port used by RADIUS changed from port 1645 to 1812. Make sure you select the policy that matches your implementation.

Characteristics

- Internet Protocol(s): UDP
- RADIUS policy Port Number(s): UDP 1645
- RADIUS-RFC policy Port Number(s): UDP 1812

RADIUS-Accounting and RADIUS-ACCT-RFC

The Remote Authentication Dial-In User Service (RADIUS) Accounting policy supplies accounting information to administrators of networks that use RADIUS authentication. RADIUS is a client-server system that keeps authentication information for users, remote access servers, and VPN gateways in a central user database that is available to all servers. The RADIUS server is also notified when the authenticated session starts and stops. This information can be helpful for accounting.

In RFC 2866, the server port used by RADIUS changed from port 1646 to 1813. Make sure you select the policy that matches your implementation.

Characteristics

- Internet Protocol(s): TCP
- RADIUS-Accounting policy Port Number(s): UDP1646
- RADIUS-ACCT-RFC policy Port Number(s): UDP 1813

RDP

The Microsoft Remote Desktop Protocol (RDP) supplies remote display and input abilities over network connections for Windows software applications that operate on a server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 3389

RIP

Routing Information Protocol (RIP) is a link state routing protocol developed in the early years of routing. Its limitations make it inappropriate for use in the Internet, but it can be useful in small networks. We recommend that you use this service only if you have enabled and configured RIP in the dynamic routing processes in the Fireware configuration.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 520

RSH

Remote Shell (RSH) is used to get access to the command line of a remote host computer. Because it is not encrypted, we do not recommend you allow any RSH incoming through the Firebox without the use of a VPN.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 514

RealPlayer G2

Media streaming protocol v7 and v8.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 554, 80

Rlogin

Remote login (RLogin) is a UNIX command that allows an approved user to log in to other UNIX computers on a network. After the login, the user can do all the operations the host has approved, such as read, edit, or delete files. Because it does not use encryption, we recommend you do not allow incoming Rlogin through the Firebox.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 513

SecurID

RSA SecurID Two-Factor Authentication give more security to the user authentication procedure. Created by Security Dynamics Technologies, Inc., it uses SecurID tokens to generate codes and ACE/Server software to corroborate the codes.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 5510, UDP 5500

SMB (Windows Networking)

Windows uses Server Message Block (SMB) to share files, computers, printers, and other network resources.

If you set up replication, you can see many tries to use the port mapper service on port 135. When this fails, SMB begins to use port 42. Refer to the RFC for DCE, and the DCE-RPC proxy sections for more instructions.

Note

SMB through the Firebox is not secure and we do not recommend it, unless used through a VPN connection. These configuration settings are to be used only if there is no other alternative, and policy settings must specify internal and external hosts.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): UDP 137, UDP 138, TCP 139, TCP 445, UDP 445

SMTP

The SMTP packet filter policy allows SMTP traffic (e-mail) without using the SMTP proxy.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 25

SNMP

Simple Network Management Protocol (SNMP) is used to collect information about and configure remote computers. This can be dangerous. Many Internet attacks use SNMP. Because SNMP can cause changes in a network if enabled, carefully review alternatives and record logs for all connections.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 161

SNMP-Trap

Simple Network Management Protocol (SNMP) traps are notification messages that an SNMP agent (for example, a router) sends to a network management station. These messages usually report an important event that must be examined.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s):162

SQL*Net

Oracle uses one port for its sql*net software. By default, this port is 1526/tcp or port 1521/tcp. Or, edit the tnsnames.ora file to change the port. To allow sql*net through the Firebox, set up a policy for the port that your sql*net server uses, with a protocol of tcp, and a client port of ignore. Then set up incoming access from the allowed external hosts to the sql*net server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1521, 1526

SQL-Server

The SQL-Server policy is used to give access to Sybase Central and SQL Advantage software.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 10000

ssh

Secure Shell (ssh) is a free application protocol that allows remote login, command control, and the movement of files between computers. It gives strong authentication and secure (encrypted) connections. We recommend the use of ssh because it is more secure than more vulnerable protocols such as telnet, rssh, and rlogin.

UNIX versions are available from www.ssh.com, and information on versions for Windows can be found at F-Secure (http://www.f-secure.com).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 22

Sun RPC

Sun Remote Procedure Call (Sun RPC) was developed by Sun Microsystems for connections between clients and servers in the Sun network file system.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 111, UDP 111

syslog

syslog is a policy used to record operating system events on UNIX hosts. Syslog data is usually enabled on a firewall to collect data from a host outside the firewall.

The syslog port is blocked in the default Firebox configuration. To allow one log host to collect logs from more than one Firebox:

- Remove port 514 from the Blocked Ports list
- Add the WatchGuard Logging policy to Policy Manager

Note

It is usually not secure to allow syslog traffic through the Firebox. It is possible for hackers to fill syslogs with log entries. If the syslog is full, it is more difficult to see an attack. Also, the disk frequently fills up and the attack is not recorded.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 514

TACACS

TACACS user authentication is a system that uses user accounts to authenticate users into a dial-up modem pool. This removes the need to keep copies of accounts on a UNIX system. TACACS does not support TACACS+ or RADIUS.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 49

TACACS+

TACACS+ user authentication is a system that uses user accounts to authenticate users into a dial-up modem pool. This eliminates the need to keep copies of accounts on a UNIX system. TACACS+ supports RADIUS.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 49

TCP

This policy serves as the default policy for all TCP connections, and other policies override it. TCP connections that do not match specified policies in Policy Manager do not complete unless TCP-UDP, TCP, or

the TCP Proxy are also configured in Policy Manager. This policy does not enable FTP, which operates only with an FTP policy.

TCP-UDP

This policy serves as the default policy for all TCP and UDP connections, and other policies override it. Connections that do not match specified policies in Policy Manager do not complete unless TCP-UDP, TCP and UDP, or the TCP Proxy are also configured in Policy Manager. This policy does not enable active mode FTP, which operates only with an FTP policy.

UDP

This policy serves as the default policy for all UDP connections, and other policies override it. UDP connections that do not match specified policies in Policy Manager do not complete unless UDP, TCP-UDP, or the TCP Proxy are also configured in Policy Manager.

telnet

The telnet policy is used to log in to a remote computer. It is almost the same as dial-up access, but the connection is made across a network.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 23

Timbuktu

Timbuktu Pro is remote control and file transfer software used to get access to Windows computers. The protocol uses TCP port 1417 and UDP port 407. Add the Timbuktu policy and allow incoming access from the hosts on the Internet that must get access to internal Timbuktu servers, and to the internal Timbuktu servers.

Timbuktu is not a very secure software application and can put network security at risk. It allows traffic inside the firewall without authentication. In addition, the Timbuktu server can receive denial-of-service attacks. We recommend that you use VPN options for more security.

Characteristics

- Internet Protocol(s): TCP, UDP
- Port Number(s): UDP 407, TCP 1417

Time

The Time policy is almost the same as NTP. It is used to synchronize clocks between hosts on a network. Time is usually less accurate and less efficient than NTP across a WAN. We recommend that you use NTP.

Characteristics

- Internet Protocol(s): TCP, UDP

- Port Number(s): TCP 37, UDP 37

traceroute

traceroute is a software application that creates maps of networks. It is used for network troubleshooting, network route troubleshooting, and finding the Internet service provider of a site. The WatchGuard traceroute policy controls UNIX-based, UDP-style traceroute only. For a DOS-based or Windows-based traceroute packet filter, use the ping policy (see "ping" on page 42).

traceroute uses ICMP and UDP packets to create paths across networks. It uses the UDP TTL field to send back packets from each router and computer between a source and a destination. If you allow traceroute incoming to a network, this can enable a hacker to create a map of your private network. But, outgoing traceroute is good for troubleshooting.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 33401-65535

UUCP

Unix-to-Unix Copy (UUCP) is a Unix tool and protocol that enables one computer to send files to another computer. This tool is not used frequently, as users more often use FTP, SMTP, and NNTP to transfer files.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 540

WAIS

Wide Area Information Services (WAIS) is a protocol you can use to find documents on the Internet. Thinking Machines Incorporated first developed WAIS. Some web sites use WAIS to look for searchable indices, but it is not used frequently.

WAIS is created on the ANSI Z39.50 search protocol, and the words Z39.50 and WAIS refer to the same technology.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 210, but servers can be (and frequently are) configured on other ports, much like HTTP servers

WinFrame

Citrix ICA is a protocol used by Citrix for its software applications, which includes the Winframe product. Winframe gives access to Windows from different types of clients. Citrix uses TCP port 1494 for its ICA protocol. Citrix MPS 3.0 uses Session Reliability by default. This changes the ICA protocol to use TCP 2598. If you use Citrix MPS, you must add a policy for TCP port 2598.

A WinFrame policy could put your network security at risk because it allows traffic through the firewall without authentication. In addition, your Winframe server can receive denial-of-service attacks. We recommend that you use VPN options to give more security for ICA connections. You can use all of the usual log options with WinFrame.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1494

WG-Auth

The WatchGuard® Authentication policy allows users to authenticate to the Firebox.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4100

WG-Firebox-Mgmt

The WatchGuard Firebox Management policy allows configuration and monitoring connections to be made to the Firebox. We recommend that you allow this policy only to the management station. The policy is usually set up on the trusted interface.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4103, 4105, 4117, 4118

WG-Logging

The WatchGuard Logging policy is necessary only if a second Firebox must get access to a log host on the trusted interface of a Firebox. If there is only one Firebox, this policy is not necessary.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4107, 4115

WG-Mgmt-Server

When you use the WatchGuard Management Server Setup wizard to configure a Management Server, the wizard automatically adds this policy to the gateway Firebox. It controls incoming connections to the Management Server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4110, 4112, 4113

WG-SmallOffice-Mgmt

The WatchGuard Small Office Management policy allows you to make a secure connection to SOHO and Edge Fireboxes from the WatchGuard System Manager.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): TCP 4109

WG-WebBlocker

The WatchGuard WebBlocker™ policy allows connections to the WebBlocker server.

Characteristics

- Internet Protocol(s): TCP, UDP
- Port Number(s): TCP 5003, UDP 5003

WHOIS

The WHOIS protocol gives information about the administrator of web sites and networks. It is frequently used to find the administrator of a different web site.

To filter WHOIS traffic, add a WHOIS policy that allows connections to the WHOIS server (such as rs.internic.net).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 43

X11

The X Windows System Protocol has components that are used to create graphic desktops, which include windows, colors, displays, and screens. X11 also supplies a flow of events that show the interaction between a user and a computer input device (such as a mouse, keyboard, and so on).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 6000-6063

Yahoo Messenger

The Yahoo Messenger Protocol is a tool for instant messaging.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 5050, 80

Proxied Policies

This section reviews the proxied policies supplied by the WatchGuard® Firebox® System. A proxy policy opens packets, strips out forbidden data types in the packet content, and assembles the packets again using the source and destination headers of the proxy.

You configure and activate proxies the same way you add packet filtering policies.

DNS

Domain Name Service (DNS) matches host names to IP addresses. The DNS proxy policy examines the contents of DNS packets to help protect your DNS servers from hackers. It puts limits on the type of operations allowed in a DNS query and can look for specified patterns in query names.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 53 and UDP 53

FTP

FTP is File Transfer Protocol. FTP is used to move files across the Internet.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 20 (command channel), 21 (data channel)

HTTP

HTTP is the Hypertext Transfer Protocol used by the World Wide Web to move information around the Internet.

Note

The WatchGuard policy "HTTP Proxy" is not the same as an HTTP caching proxy. An HTTP caching proxy controls the caching of Web data. If you use an external caching proxy, you must enable (by adding policies) any outgoing policies that are necessary for your organization. If you do not, outgoing TCP connections do not operate correctly.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 80 (but servers can operate on any port, a common alternative is 8080, and Secure Socket Layer (SSL) connections are usually served on port 443)

SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet standard protocol used to transmit and receive e-mail. Usually SMTP servers are public servers.

You must add an auth policy to Policy Manager when you use incoming static NAT with SMTP (see "auth" on page 32). Configure auth to allow incoming auth to the Firebox. This enables outgoing mail

messages to flow freely from behind the Firebox to the many SMTP servers on the Internet that use auth. It allows these servers to send messages back through the Firebox to the senders.

Logging incoming SMTP is recommended, but this can cause a large quantity of logs. To not use the SMTP proxy but have SMTP operate correctly, create a new policy in Policy Manager that uses TCP protocol and port 25.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 25

TCP Proxy

The TCP Proxy policy gives configuration options for HTTP on port 80 and adds a rule that allows TCP connections from networks behind the Firebox to networks external to the Firebox by default. The TCP Proxy rule makes sure that all HTTP traffic from behind the Firebox on all ports is proxied with the HTTP proxy rules.

We recommend that you allow HTTP only to any public HTTP servers kept behind the Firebox. External hosts can be spoofed. WatchGuard cannot make sure that these packets were sent from the correct location.

Configure WatchGuard to add the source IP address to the Blocked Sites list when an HTTP connection to a host behind your Firebox is denied. Configure the parameters and MIME types the same as you do for the HTTP Proxy.

Index

Symbols

.cfg file. See configuration file
.ftr files 192
.wgl files
  converting to .xml format 95
  described 91

Numerics

1-1 Mapping dialog box 118
1-to-1 NAT. See NAT, 1-to-1

A

Activate Gateway AntiVirus wizard 309
Activate Intrusion Prevention wizard 314–315
Activate spamBlocker wizard 302
Activate WebBlocker wizard 291–293
active connections on Firebox, viewing 53
Active Directory authentication 131
active features, viewing 60
Add Address dialog box 119, 152, 155, 249, 281
Add Alias dialog box 74
Add Device wizard 214
Add Dynamic NAT dialog box 115
Add Event Processor dialog box 84
Add Exception Rule dialog box 304
Add Firebox Group dialog box 125
Add Firebox License Key dialog box 59, 301
Add Policies dialog box 147
Add Policy wizard
  adding custom Edge Configuration Templates with 270
  adding existing Edge Configuration Templates with 269
Add Protocol dialog box 149, 271
Add Route dialog box 110, 111
Add Search Rule dialog box 93
Add Site dialog box 138
Add Static NAT dialog box 120, 155
Add User or Group dialog box 132
Add VPN wizard 240, 264
Add WebBlocker Server dialog box 294
Advanced Diagnostics dialog box 86
Advanced Encryption Standard (AES) 227
advanced rules view (in Proxy definitions) 163
Advanced Settings dialog box 111
AH (Authentication Header) 226
alarms
  and FTP 174
  configuring 164
  configuring for DNS proxy 182
  configuring for proxy rules 164
  configuring proxy and antivirus 171
  described 163
  for Gateway AntiVirus responses 311
aliases
  and managed Firebox X Edge devices 275
  creating 74
  default 73
  defining on Firebox X Edge 277
  described 73
  for IP addresses 21
  naming on Management Server 276
Aliases dialog box 74, 276
allow (proxy action) 162
anonymizer web sites 293
ANSI Z39.50 396
Antispyware Blocklist Categories dialog box 139
Any policy
  and precedence 158
  and RUVPN 284
  described 379
Any-External alias 73
Any-Optional alias 73
Any-Trusted alias 73
AOL policy 380
Archie policy 380
ARP cache, flushing 40
ARP table, viewing 49
attacks

about SYN flood setting 137
address space 137
DDoS 137
Denial of Service (DoS) 137
flood 137
IPsource route 136
Ping of death 136
port space 137
stopping 135–138
auth (ident) policy 380
authentication
Active Directory 131
and ssh 393
defining groups for 123
described 74, 121, 227
for VPNs, viewing 6
from external interface 122
from outside Firebox 122
MD5-HMAC 227
of remote users 124
selecting method for 227
setting idle time-out for 77
SHA-HMAC 227
through Firebox to other Firebox 122
using external server 227
Authentication Header 226
authentication idle time-out, setting 77
Authentication List tab (Firebox System Manager) 49
authentication servers
and policies 132
configuring Fireboxes as 125
described 227
LDAP 129
RADIUS 127
SecurID on RADIUS server 128
types of 123
types supported 281
using backup 123
using Fireboxes as 123
Authentication Servers dialog box 125, 282
Auto Adjustment setting, TCP segment size 77

B

Backup dialog box 73
backup images
creating 72
described 72
restoring 73
backup of configuration file 14
Bandwidth Meter tab
adding/removing lines in 46
changing colors in 46
changing interface names in 46
changing scale of 45
described 45
bandwidth usage, viewing 45
base encryption 14
block (proxy action) 162
blocked ports
avoiding problems with legitimate users 143
blocking sites that use 143
default 142
logging and notification for 143
permanent 143
reasons for 142
Blocked Ports dialog box 143
Blocked Ports list 143
blocked sites
adding from HostWatch 55
auto-blocked 138
blocking with policy settings 141
described 138
dynamic 141
exceptions to 140
logging and notification for 140
permanent 138
spyware sites 139
storing in external file 140
temporary 141
viewing current 49
Blocked Sites Configuration dialog box 138
Blocked Sites list
adding/removing sites from 50
and Gateway AntiVirus 311
described 138
exceptions to 140
using proxy definitions for 162
viewing 50
Border Gateway Protocol (BGP)
allowing traffic through Firebox 341
configuring Fireware to use 340
daemon configuration 338–339
described 337, 380
BOVPN
and certificate-based authentication 233
described 233
multi-WAN not supported in 102
BOVPN with Manual IPSec
adding gateways 243
and strong encryption 14
configuring a gateway 243
configuring a tunnel with manual security 246
creating tunnel policies 250
described 233, 243
encryption levels for 233, 243
listed on Device Status tab 220
outgoing dynamic NAT and 250
Phase 1 settings 245
specifying authentication method 245
specifying encryption type 245
BOVPN with WatchGuard System Manager
adding policy templates 237
adding security templates 239
creating tunnels 240
defining Fireboxes as managed clients 237
described 233
editing tunnels 241
listed on Device Management tab 220
removing devices/tunnels 241
scenario 234
Branch Office IPSec Tunnels dialog box 246
branch office VPN. See BOVPN

C

CA. See Certificate Authority
cables, installing 22
Certificate Authority
configuring certificate for 201
described 201, 221, 228
managing 222
recording diagnostic log messages for 204
Certificate Revocation List (CRL)

configuring properties for 203, 204
described 221
publishing 223
certificates
described 227, 228
destroying 223
generating new 223
listing current 223
printing to the screen 223
reinstating 223
revoking 223
searching for 223
viewing CA fingerprint 37
viewing expiration date and time of 37
viewing status of 36
Change Passphrases dialog box 65
Citrix ICA policy 380
Clarent-command policy 381
Clarent-gateway policy 381
clock, synchronizing to NTP server 61
configuration file
and Policy Manager 69
backing up 14
customizing 19
making a new 71
opening 69
opening local 71
saving 71
saving to Firebox 72
saving to local drive 72
configuration modes, described 11
configuration passphrase
changing 64–65
described 18, 64
setting 16
Configure Log Servers dialog box 84
Configure Syslog dialog box 84
Configure WINS and DNS screen 258
Connect to Device dialog box 18
Connect to Firebox dialog box
described 31
troubleshooting 70
connection status, viewing 6
Connections For dialog box 53
cookies 177
CPU use, graphing 41
CRL. See certificate revocation list
CU-SeeMe policy 382
custom idle time-out for policies, setting 157

D

DDoS attacks 137
default gateways
and drop-in configuration 12
for secondary private networks 21
viewing IP address of 6, 36
default packet handling
and address space attacks 137
and address space probes 137
and DDoS attacks 137
and Denial of Service (DoS) attacks 137
and flood attacks 137
and IP source route attacks 136
and Ping of death attacks 136
and port space attacks 137
and port space probes 137
and spoofing attacks 136
described 135
options for 135
Default Packet Handling dialog box 135–138
Denial of Service (DoS) attacks 137
deny (proxy action) 162
deny message, changing default 171
Device Configuration dialog box 62
Device Management Page
described 216
for Firebox 216, 218
for Firebox X Edge 217
starting other tools from 219
updating device 218
VPN resources 219
VPN tunnels 220
Device Management tab
and managed VPNs 220
configuring settings on 216
described 5
removing a device from 241
starting other tools from 219
Device Policy dialog box 239
Device Properties dialog box 218, 262, 266
Device Status tab
and BOVPN with Manual IPSec 220
described 4, 5
removing a device from 241
devices, removing from WatchGuard System Manager 241
devices. See also Firebox, SOHO, etc.
DHCP 99
DHCP relay, configuring 99
DHCP server
configuring Firebox as 99
default lease time for 99
described 99
using for external interface addressing 101
using server remote from client 99
DHCP support on external interface 21, 100
DHCP-Server policy 382
diagnostic log file, setting location for 49
diagnostic logging
described 90
for Certificate Authority 204
for Management Server 201
selecting level of 85
Diffie-Hellman groups
changing settings 245
described 228, 245
digital certificates. See certificates
DMZ (Demilitarized Zone) 11
DNS
policy for 382
DNS proxy
adding new query types rules 182
and Intrusion Prevention Service 314, 319
and intrusion protection 182
configuring 180–182
configuring alarms 182
configuring DNS query names 182
configuring DNS query types 181
configuring general settings for 180
described 180, 399
OPcodes, configuring 181
DNS servers
addresses for 107

configuring 280
Domain Name System. See DNS
Don't Fragment bit, ignoring heading of 75
Download WebBlocker Database dialog box 290
drop (proxy action) 162
drop-in configuration
characteristics of 13
configuring related hosts 111
described 11, 12
multi-WAN not supported in 13, 102
Drop-In Mode Properties dialog box 112
duplex parameters, setting 111
DVCP Server. See Management Server
dynamic DNS
creating a DynDNS account 108
described 108
setting up Firebox for 109
dynamic NAT. See NAT, dynamic
dynamic routes, viewing 49
dynamic routing
described 323, 326
protocols for 323, 326
routing daemon configuration files 326
using Border Gateway Protocol (BGP) 337–341
using OSPF 332–337
using RIP (Routing Information Protocol) 326
using RIP (Routing Information Protocol) V1 326–330
using RIP (Routing Information Protocol) V2 330–332
viewing components of 49
Dynamic Routing Setup dialog box 328, 331, 335, 340
dynamically blocked sites 141
DynDNS account, creating 108

E

Edge Configuration Templates
adding with Add Policy wizard 269–271
applying to devices 271–273
cloning 271
creating/applying 268–269
described 268
Edge Network Settings dialog box 274
Edit Gateway dialog box 246
Edit Policy Properties dialog box 79, 156, 208
Edit Service Properties dialog box 210
Edit Tunnel dialog box 249
e-mail addresses, setting maximum length for 167
e-mail attachments, limiting file names for 170
e-mail messages 171
actions for attachments 311
and the SMTP proxy 166
as notification 89, 153, 165
creating rules for bulk or suspect 304–305
hiding server data for 168
restricting recipients 170
restricting senders 170
scanning compressed attachments in 312
setting maximum line length for 168
setting maximum recipients for 167
setting maximum size for 167
setting responses for viruses in 170
spam. See spamBlocker
unlocking attachments 312
Enable TOS for IPSec option 76
Encapsulated Security Payload 226
encryption
Advanced Encryption Standard (AES) 227
and BOVPN with Manual IPSec 233
and management software 14
and RUVPN with PPTP 279
and VPNs 226–227
base, described 14
described 226
for VPNs, viewing 6
levels of 227
strong, activating 279
strong, and BOVPN with Manual IPSec 14
strong, described 14
encryption key
for creating backup image 73
log. See log encryption key
Entrust policy 382
ESMTP
configuring authentication rules 169
configuring parameters for 169
described 168
extended authentication
defining groups for 281
described 227
external interface
configuring 100–102
configuring multiple. See multi-WAN support
described 10
dynamic addressing on 100
dynamic IP support on 21
using a static IP address for 100
using DHCP for addressing 101
using PPPoE on 100

F

FAQs 26
fbxinstall utility 66
feature keys 58
features, activating 57
file locations for 377
File Transfer Protocol. See FTP proxy
finger policy 383
Firebox Installation Services 29
Firebox interfaces
changing address of 98
configuring 98–110
described 11
monitoring traffic through 35
see also individual listings for interfaces
viewing IP addresses of 5, 36
Firebox License Keys dialog box 59, 289
Firebox passphrases. See passphrases
Firebox running Fireware, configuring as managed client 208
Firebox running WFS, configuring as managed client 210
Firebox System Manager
and Intrusion Prevention Service 321
Authentication List tab 49
Bandwidth Meter tab 45
Blocked Sites list 50
described 2, 18, 31
Firebox and VPN tunnel status 36
front panel 36
Front Panel tab 34
menus and toolbars in 32
monitoring spamBlocker activity with 305

monitoring tunnels in 37
opening 32
pausing 34
Performance Console 40–44
Security Services tab 51, 306, 313, 321
Service Watch tab 46
setting refresh interval for 34
star display 35
starting 31
Status Report tab 48–49
Traffic Monitor tab 38–40
triangle display 35
viewing bandwidth usage 45
viewing Firebox status 48
viewing Firebox traffic 35
viewing Gateway AntiVirus status 313
Firebox X Edge
adding to Management Server 257–259
adding VPN resource 263
adding VPN tunnel 264
configuring as managed client 211
configuring management properties for 262
creating tunnels for dynamic 240
defining aliases on 277
importing into Management Server 255
managing 253–259
managing network settings 273–275
modifying configuration template for 265
preparing installed device for management 255
preparing new unit for management 254
scheduling firmware updates for 259–260
starting tools for 264
updating device 263
using aliases with 275
viewing management page for 261
Firebox X e-Series
and Web Quick Setup Wizard 15
High Availability and 344–346
resetting 65
Fireboxes
as Certificate Authorities 228
backup image of 72
cables for 22
configuring as DHCP server 99
configuring for RUVPN with PPTP 279
configuring management properties for 218
configuring to accept SNMP polls 62
connecting to 17, 31
defining as managed clients 237
designating Log Server for 83
disconnecting from 18
friendly names in log files, reports 62
global settings 75
hosting PPTP sessions 124
interfaces. See Firebox interfaces
making outbound PPTP connections from behind 287
managing from remote location 78
monitoring status 31
obtaining IP addresses dynamically 21
opening configuration file 69
package contents 9
recovering 65
resetting passphrases 64
resetting to factory-default 65
resetting using fbxinstall 66
saving configuration file to 72
setting time zone for 62
synchronizing clock to NTP server 61
timeout value 18, 208
using as authentication servers 123
viewing active connections on 53
viewing ARP table for 49
viewing bandwidth usage 45
viewing kernel routing table for 49
viewing load average of 48
viewing memory use of 48
viewing model of 48
viewing network card information 49
viewing processes of 49
viewing status of 48
viewing traffic and performance 48
viewing traffic through 35
Fireware
described 1
differences between Fireware/Fireware Pro 2
upgrading 20
Fireware Pro
described 1
differences between Fireware/Fireware Pro 2
firmware updates, viewing/deleting 261
flood attacks 137
Fragmentation Req (PMTU) setting (ICMP) 76
Front Panel tab (Firebox System Manager) 34
FSM. See Firebox System Manager
FTP policy 383
FTP proxy
and Intrusion Prevention Service 173, 314, 319
configuring general settings 172
configuring proxy alarms for 174
defining commands rules for 173
described 172, 399
setting download rules for 173
setting upload rules for 173
FTP servers, and archie policy 380
fully meshed topology 229

G

Gateway AntiVirus
actions (Allow, Drop, Block, Lock, Remove) 311
activating 309
and the HTTP proxy 308
and the SMTP proxy 308
applying settings to policies 309
configuring 310–313
configuring engine settings for 311
configuring signature server for 312
creating alarms/logs for 311
described 307, 308
enabling automatic virus signature updates 312
installing 308
unlocking an attachment 312
updating antivirus software 314
updating signatures manually 314
using with multiple proxies 312
viewing engine version 52
viewing information on 51
viewing recent activity 52
viewing signature information 52
viewing status of 313
Gateway AntiVirus dialog box 310, 311
gateways
default. See default gateways
described 243
for tunnels, adding 243
for tunnels, configuring 243–246

for tunnels, editing/deleting 246
selecting for tunnel 247
Gateways dialog box 244
Generic Routing Encapsulation Protocol (GRE)
policy 383
global settings
for authentication 77
for ICMP error handing 76
for TCP SYN checking 76
for VPNs 75
TCP segment size 77
using for Firebox 75
Global Settings dialog box 75
gopher policy 383
groups (authentication)
assigning users to 126
components of 123
described 123, 282

H

HELO/EHLO responses, examining 168
High Availability (HA)
and Intrusion Prevention Service 348
and proxy sessions 348
backing up configuration 348
configuring (Firebox X e-Series) 344–346
configuring (non e-Series) 346–347
configuring secondary Firebox (Firebox X e-Series) 345
described 3, 343
enabling (Firebox X e-Series) 345
forcing a failover 347
Gateway AntiVirus and 348
requirements for 343
restarting the peer 347
selecting primary Firebox for 344
synchronizing the configuration 347
upgrading software in HA configuration 348
viewing status of 36
High Availability dialog box 344, 346
Historical Reports
and SMTP traffic 168
applying a filter 193
automating reports with Log Server 88
creating report filter 192
creating/editing 185–190
deleting a filter 193
deleting reports 187
described 19, 185
editing a filter 192
editing existing reports 187
running a report 193
starting 185
starting new reports 186
time spans for 187
time zone for 62
Home Banking Computer Interface (HBCI) policy 384
host routes, configuring 110
Host Unreachable setting (ICMP) 76
hosts
related, configuring 111–112
viewing in HostWatch 54
HostWatch
adding blocked sites from 55
changing view properties 55
choosing colors for display 55
described 18, 53
display 53
pausing 56
setting display properties 54
starting 53
viewing authenticated users 54
viewing hosts 54
viewing ports 54
HTTP caching proxy 399
HTTP policy 384, 399
HTTP proxy
and antivirus responses 178
and Gateway AntiVirus 308, 310
and Intrusion Prevention Service 314, 315, 317
and range requests 175
and WebBlocker 292
changing deny message 178
configuring settings for requests 174
described 174, 399
sending log messages per transaction 175
setting body content types 178
setting content types for responses 177
setting cookies for responses 177
setting header fields for responses 177
setting HTTP request URL paths 176
setting idle timeout for 175, 177
setting length of response headers 177
setting maximum line length of response headers 177
setting maximum URL length 175
setting request authorization 176
setting request header fields 176
setting request methods 175, 177
HTTPS policy 384
hub-and-spoke configuration 230

I

ICMP error handling settings
for Firebox 76
in policies 157
Identification Protocol (IDENT) policy 384
idle time-out for policies, setting 157
IGMP policy 385
Ignore DF for IPSec setting 75
IKE
and Diffie-Hellman group 245
and Phase 1 settings 245
described 228
phase 1,2 228
IKE policy 385
IMAP policy 385
installation procedures 9–22
Instant Messaging (IM) use, preventing 317
Intel Video Phone policy 386
Interface Settings dialog box 98, 106
interfaces
changing IP address of 98
configuring 98–110
graphing events on 41
setting speed and duplex 111
viewing configuration of 49
Internet
accessing through PPTP tunnel 286
security concerns on 225
threats from hackers on 171, 307, 314
virus traffic on 24

Internet Group Management Protocol (IGMP) policy 385
Internet Key Exchange. See IKE
Internet Mail Access Protocol (IMAP) policy 385
Internet Relay Chat (IRC) policy 386
Internet Security Association and Key Management Protocol 246
Intrusion Prevention dialog box 316, 320, 321
Intrusion Prevention Service
activating 314–315
and DNS proxy 314, 319
and FTP proxy 314, 319
and High Availability 348
and HTTP proxy 314, 315, 317
and SMTP proxy 319
and TCP proxy 314, 315, 317
configuring 316–321
configuring signature exceptions 320
configuring signature server 320
copying settings to other policies 320
creating new proxy policies 315
described 307, 314
enabling automatic virus signature updates 320
installing 308
intrusion severity levels 316
selecting proxy policies to enable 315
updating signatures manually 322
viewing information on 51
viewing recent activity 52
viewing signature information 52
viewing status of 321
intrusion severity levels (High, Medium, Low) 316
intrusions
described 307
see also Intrusion Prevention Service
viewing number found 37
IP addresses
and routed configuration 12
and VPNs 228
default gateways 6, 36
entering 22
entering for RUVPN with PPTP 281
netmask 6, 36
of Firebox interfaces 36
WINS/DNS servers 108
IP alias 21
IP source route attacks 136
IPS. See Intrusion Prevention Service
IPSec
and BOVPN with Manual IPSec 233
and BOVPN with WatchGuard System Manager 233
benefits of 226
described 226
encryption method for 227
pass through setting 75
policy for 385
setting global parameters for 75
types of tunnels that use 6, 37
IRC policy 386
ISAKMP
and Diffie-Hellman groups 245
described 246

K

Kerberos policies 386
kernel routing table, viewing 49
key pairs 221
known issues 26

L

L2TP policy 386
launch interval, setting 141, 153, 165
LDAP
policy for 386
LDAP authentication 129–130
LDAP-SSL policy 387
license key certificates 10
license keys
adding 59
deleting 59
described 57
downloading 61
seeing properties of 61
viewing 60
Licensed Features dialog box 301, 308
Limit to setting, TCP segment size 77
link speed, setting 111
LiveSecurity Gold Program 29
LiveSecurity Service
activating 25
benefits of 23
broadcasts 24
described 19
Rapid Response Team 24
technical support 28
load average of Firebox, viewing 48
Local Alias Setting dialog box 278
Local-Remote Pair Settings dialog box 249
lock (proxy action) 163
log encryption key
changing 82
default 16
setting 82
setting for new servers 84
log files
consolidating 95
converting from .wgl to .xml format 95
copying entries 94
creating a search rule 93
default location for 90
merging 95
names of 90
searching 94
setting Firebox names used in 62
setting location for diagnostic 49
setting rollover frequency for 87
setting size for 87
viewing with LogViewer 90
log messages
blocking source/destination of 40
configuring for proxies 164, 165
configuring for rules 164, 165
copying address of 40
copying to another application 39
pinging source/destination 40
sending for HTTP transactions 175
setting maximum number of 38
showing in color 39
tracing route to 40
Log Servers
adding 83
and log files 90
and reports 185

automating reports using 88
changing encryption key for 82
described 1, 82
icon on toolbar for 4
installing on computers with desktop firewalls 20
locations for 81
setting designated for Firebox 83
setting priority for 84
setting up 82
starting/stopping 89
viewing IP addresses of 48
where to install 13
logging
alarm log messages 90
configuring for policies 153
configuring for proxies 164
described 81, 89
diagnostic log messages 90
enabling advanced diagnostics 85
enabling syslog 84
event log messages 90
for blocked ports 140, 143
Gateway AntiVirus responses 311
global preferences for 86
spamBlocker responses 304
traffic log messages 90
where to view messages 89
Logging and Notification dialog box 140, 153, 164
Logging Setup dialog box 83, 84, 85
LogViewer
copying log data 94
creating a search rule 93
described 19, 91
exporting log file data 94
resetting to default colors 92
searching by keyphrase 92
searching for entries 94
seeing sample log message 92
selecting columns to display 92
setting background color 92
setting color for message type 92
setting preferences 92
showing logs 92
showing messages in color 92
starting 91
time zone for 62
viewing current file in 94
viewing files with 90
Lotus Notes policy 387

M

MAC addresses
of interfaces, viewing 6, 36
stored on Firebox 40
main menu button 40
managed client
configuring Firebox running Fireware as 208
configuring Firebox running WFS as 210
configuring Firebox X Edge as 211
defining Firebox as 237
described 208
enabling to send log messages 209
SOHO 6 as 212
Managed Client Setup dialog box 209
Management Information Bases, location of 64
Management Page
described 216
for Firebox 216, 218
for Firebox X Edge 217, 261–265
starting other tools from 219
updating device 218
VPN resources 219
VPN tunnels 220
Management Server
adding devices to 213–216
adding Edge/SOHO devices to 257–259
adding/removing license for 200
and Firebox X Edge 254
and SOHO 254
and VPN Manager 233
as Certificate Authority 222
backing up/restoring configuration of 204, 205
changing configuration of 200
connecting to 207
creating new 199
described 1, 197
Device Management page. See Device Management page
disconnecting from 208
icon on toolbar for 4
importing Firebox X Edge devices into 255
license keys for 201
managing devices with 208–213
master encryption key 197
moving to a new computer 205
naming aliases on 276
passphrase 198
passphrases for 197
recording diagnostic log messages for 201
using only to monitor 208
using Setup wizard 199
where to install 13
Management Server Backup/Restore Wizard 205
Management Server Configuration dialog box 200
Management Server settings page 259, 276, 277
management station
and software encryption levels 14
setting up 13
master encryption key
described 197, 198
setting 199
when to use 198
MD5-HMAC 227
memory use of Firebox, viewing 48
Merge Logfiles dialog box 95, 96
meshed topology 229
MIBs, location of 64
Microsoft SysKey Utility 198
Mobile User VPN. See MUVPN
MS Win Media policy 387
MSDUN, and RUVPN 285
MSSQL-Monitor policy 387
MSSQL-Server policy 387
multi-WAN support
and NAT 102, 119, 157
and network configuration 13
and QoS actions 325
described 3, 102
in round-robin order 102
limitations of 102
routing table option 103
MUVPN
and certificates 222
and WINS/DNS server addresses 107
authentication for 232

configuring Firebox to host 124
described 232
encryption levels for 232
monitoring tunnels 220
multi-WAN not supported in 102
scenario 235
with extended authentication 235
MUVPN tunnels, seeing information on 37
MX records 154

N

NAT
1-to-1
and PPPoE support 22
and VPN tunnels with same IP address 117
configuring 118
configuring policy-based 118, 119
defining rules for 117
described 113, 116
not supported in multi-WAN 102
using 116
using in policies 156
and tunnel switching 231
and VPNs 229
described 2, 113
dynamic
adding entries 114
allowing through BOVPN tunnel 250
changing entry order 115
described 113, 114
enabling 114
policy-based 115
using in policies 119, 156
static
configuring a policy for 154
configuring for a policy 119
described 113
types of 113
NAT Setup dialog box 114
NAT Traversal 245
netmask, viewing address of 6, 36
NetMeeting policy 388
network address translation. See NAT
network cards, viewing information about 49
Network Configuration dialog box 98, 99, 104, 106, 112
Network Connection wizard 285, 286
Network File System 142
Network File System (NFS) policy 388
network routes. See routes
Network Time Protocol (NTP) policy 388
Network Time Protocol server, synchronizing Firebox clock to 61
network topology
fully meshed 229
hub-and-spoke 230
partially meshed 230
Network Unreachable setting (ICMP) 76
networks, secondary. See secondary networks
New Gateway dialog box 244, 250
New Policy Properties dialog box 148
New Policy Template dialog box 149
New QoS dialog box 324
New Schedule dialog box 78
New Tunnel dialog box 247
NFS policy 388
NNTP policy 388
No Adjustment setting, TCP segment size 77
notation, slash 22
notification
bringing up popup window as 141, 153
configuring for proxies 164
for blocked ports 140, 143
global preferences for 86
sending 165
sending e-mail messages for 89
setting launch interval 141, 153, 165
setting repeat count 141, 153, 165
NTP policy 388
NTP server, synchronizing Firebox clock to 61
NTP Setting dialog box 61

O

Online Help 27
online support services
accessing 26
described 25
online training 26
Open Firebox dialog box 65, 70
optional interface
and DHCP 99
and DHCP relay 99
configuring 98–100
described 11
OSPF (Open Shortest Path First)
allowing traffic through the Firebox 336
configuring Fireware to use 335
daemon configuration 332
described 332
Interface Cost table 334
OSPF policy 389

P

packet filter policies. See policies
packet filters 145
packet handling, default. See default packet handling
packets
unhandled 137
viewing number sent and received 6, 36
partially meshed networks 230
passphrases
and SysKey utility 198
authentication 227
changing 64
configuration, changing 64
configuration, described 18
described 227
for authenticating to Firebox 126
location of 198
Management Server 198
resetting for Firebox 64
setting in Quick Setup Wizard 16
status, changing 64
status, described 18
tips for creating 64
types of 64
passwords
and security of VPN endpoints 227
file containing 198

PCAnywhere policy 381, 389
Peer to Peer (P2P) use, preventing 318
Per Interface Dynamic DNS dialog box 109
Perfect Forward Secrecy 248
Performance Console
  adding a new chart to 44
  changing polling interval for 44
  defining counters for 41
  deleting a chart 44
  described 40
  monitoring VPN events 41
  multiple graphs 44
  showing events of selected policies 41
  showing interface events 41
  showing system information 41
  viewing graph 43
PFS 248
Phase 1
  described 228
  settings 245
Phase 2
  changing settings 247
  described 228
Phase1 Advanced Settings dialog box 245
Phase2 Advanced Settings dialog box 248
Phase2 Proposal dialog box 247
ping command for source of messages 40
Ping of death attacks 136
ping policy 389
PKI 221
Point to Point Tunneling Protocol. See PPTP
Point-to-Point Protocol over Ethernet. See PPPoE
policies
  adding 147
  adding several of same type 150
  and your security policy 19
  changing properties of 150–157
  configuring for incoming static NAT 154
  configuring notification for 153
  configuring static NAT for 113, 119
  configuring to allow RUVPN traffic 283
  creating 145–157
  creating custom 148
  deleting 150
  described 145
  graphing events regarding 41
  ICMP error handling in 157
  setting destinations for 151
  setting logging properties for 153
  setting precedence for 157–159
  setting schedules for 156
  setting sources for 151
  setting time-out for 157
  types of 379
  user authentication and 132
  versus proxies 161
  viewing icons for 146
  viewing number of connections by 46
  well-known 379
Policy Manager
  as view of configuration file 69
  described 2, 18, 69
  displaying detailed view 147
  displaying Large Icons view 146
  opening a configuration file from 69
  using to modifying configuration file 97–102
Policy Properties dialog box 164
policy templates
  adding 237
  adding resources to 239
  creating new 238
  getting current 238
policy-based 1-to-1 NAT 118, 119
policy-based dynamic NAT 115
POP2 policy 389
POP3 policy 389
popup window, as notification 141, 153, 165
port space probes 137
Port Unreachable setting (ICMP) 76
ports
  blocking 142–143
  monitoring 54
  restricting for MUVPN clients 124
  specifying for policies 150
  speed and duplex settings 111
  viewing in HostWatch 54
PPP user name and password 21
PPPoE
  and 1-to-1 NAT 21
  described 100
  setting parameters for 101
  support on external interface 21, 100
PPPoE parameters dialog box 101
PPPoE support on external interface 100
PPTP
  described 226
  policy for 390
  See also RUVPN with PPTP
  VPN tunnels, seeing information on 37
PPTP_Users group, adding new users to 282–283
private LAN 10
processes, viewing information on 49
processor load indicator 36
Properties dialog box 141
Protocol Unreachable setting (ICMP) 76
Provide Contact Information screen 258
proxied policies. See proxies
proxies
  advanced rules view 163
  and Gateway AntiVirus 3
  and Intrusion Prevention Service 3
  associated multiple actions with 161
  categories list 161
  configuring 161–183
  configuring logging/notification for 164
  described 145, 161
  preconfigured 145
  See also individual names of proxies
  versus packet filters 161
proxy rules. See rules
Public Key Intrastructure (PKI) 221

Q

QoS Actions dialog box 324
Quality of Service (QoS)
  applying actions to policies 156, 325
  creating actions for 323–325
  described 3, 323
  using in a multi-WAN environment 325
Quick Setup Wizard
  described 14
  launching 16
  non-Web 16

Web
described 15
troubleshooting 15
using 15
using for recovery 15

R

RADIUS policy 390
RADIUS server authentication 127
RADIUS-Accounting policy 390
Rapid Response Team 23, 24
rcp 142
RDP policy 390
RealPlayer G2 policy 391
recovery
and Web Quick Setup Wizard 15
procedure for 65
red exclamation point in WatchGuard System Manager 7
refresh interval for Firebox System Manager 34
related hosts, configuring 111
Remote Desktop Protocol (RDP) policy 390
remote location, managing Firebox from 78
Remote Proxies category (WebBlocker) 294
repeat count, setting 141, 153, 165
Report Filter dialog box 192
Report Properties dialog box 186, 187, 188, 189, 190
reports
and network interface relationships 190
applying a filter 193
authentication details 193
automating with Log Server 88
backing up 187
consolidating sections 189, 193, 196
creating filters 192
creating/editing 185–190
deleting 187
deleting a filter 193
denied incoming/outgoing packet detail 195
denied packet summary 195
denied service detail 195
described 185
detail sections 190
editing 187, 188
editing filters 192
exporting to HTML 191
Firebox statistics 193
FTP detail 195
host summary 194
HTTP detail 194
HTTP summary 194, 196
including DNS names for IP addresses 189
location of 190
NetIQ format 191
network statistics 196
proxy summary 194
running 193
sections in 188, 193
service summary 194
session summary 194
setting Firebox names used in 62
SMTP summary 194
specifying sections for 188
starting new 186
summary sections 190
time spans for 187
time summary 194, 196
using filters 191
viewing list of 187
WebBlocker detail 195
Resource dialog box 239
RIP (Routing Information Protocol)
described 326, 391
Version 1
allowing broadcasts through Firebox 329
configuring Fireware to use 328
described 326
Version 2
allowing multicasts of 331
configuring Fireware to use 331
described 330
RIP policy 391
rlogin 142
Rlogin policy 391
root certificate, publishing 222
round-robin order, multiWAN 102–103
routed configuration
characteristics of 12
described 11
routes
configuring 110
described 110
host 110
network 110
viewing 49
RPC portmapper 142
rsh 142
RSH policy 391
rules
changing precedence of 163
components of 161
configuring alarms for 164
configuring log messages for 164
rulesets
adding 162
and advanced rules view 163
categories of 161
described 161
RUVPN with PPTP
accessing the Internet with 286
activating 281
and MSDUN 285
and the Any policy 284
and WINS/DNS server addresses 107
configuration checklist 279
configuring policies to allow 283
configuring shared servers for 280
described 232, 279
encryption levels 279
entering IP addresses for 281
IP addressing 279
making connections from behind Firebox 287
preparing client computers for 284
preparing Windows 2000 remote host 286
preparing Windows XP remote host 285
running 286

S

Save to Firebox dialog box 72
schedules
creating 77
described 77

for WebBlocker actions 297
using for policies 156
Schedules dialog box 77
secondary networks
adding 21, 105
and Web Quick Setup Wizard 21
described 21
Secondary Networks dialog box 107
SecurID authentication 128
SecurID policy 392
security policy
customizing 19
described 19
See also configuration file
Security Policy dialog box 240
Security Services tab (Firebox System Manager) 51
Security Template dialog box 239, 241
security templates
adding 239–240
described 237, 239
Select Device dialog box 273
Select Firebox Model and Name dialog box 71
Select the Time and Date page 260
service properties, using to block sites 141
Service Watch tab
adding/removing lines in 47
changing colors in 47
changing policy names in 47
changing scale of 47
described 46
showing connections by policy/rule 47
Settings dialog box 38, 92
Setup Firebox User dialog box 126, 283
Setup Routes dialog box 110
SHA-HMAC 227
shared secrets 227
Simple Mail Transfer Protocol 399
Simple Network Management Protocol. See SNMP
sites, blocked. See blocked sites.
slash notation 22
SMB policy 392
SMTP packet filter policy 392
SMTP proxy
and Gateway AntiVirus 308, 310
and intrusion prevention 171
and Intrusion Prevention Service 314, 319
and spamBlocker 302
configuing proxy/antivirus alarms 171
configuring 166–172
configuring authentication rules 169
configuring content filtering 170
configuring ESMTP parameters 168
configuring general settings 167
defining antivirus responses 170
defining content type rules 170
defining file name rules 170
described 166, 399
examining HELO/EHLO responses 168
hiding e-mail server data 168
idle timeout for 167
logging connection requests through 168
restricting e-mail senders/recipients 170
setting maximum e-mail recipients 167
setting values for header filtering 170
with static incoming NAT 384
writing custom deny message 171
SNMP
configuring Firebox to accept polls from server 62
described 62, 392
enabling polling for 63
management system 165
policy for 392
SNMP Settings dialog box 63
SNMP traps
configuring for default packet handling 136
enabling 63
enabling for policies 153
sending 165
SNMP-Trap policy 393
software upgrades
and High Availability 348
and LiveSecurity Service 19, 24
and Quick Setup WIzard 14
Fireware 20
software version, viewing 48
SOHO
creating tunnels for dynamic 240
managing 253
SOHO 5, managing 253
SOHO 6
adding a VPN resource 267
adding a VPN tunnel 268
adding to Management Server 257–259
as managed client 212
configuring management properties for 266
preparing for management 256
starting tools for 267
updating device 266
viewing management page for 265
spam messages
and reverse lookup of source IP 154
viewing number blocked 37
spamBlocker
actions (Deny, Tag, Allow) 299
actions, selecting 302
activating 301–302
adding exceptions 304
adding tags to e-mail subject line 300
categories (Spam, Bulk, Suspect) 300
configuring 303–304
creating proxy policies for 302
customizing using multiple proxies 306
described 171, 299
installing license for 300
logging responses 304
monitoring activity of 305
reporting false positives/negatives 305
selecting policies for 302
viewing recent activity 53
spamBlocker dialog box 303
speed and duplex parameters, setting 111
split tunneling
and security 232
with PPTP, enabling 286
spoofing attacks 136
spyware sites, blocking 139
spyware, blocking 318
SQL*Net policy 393
SQL-Server policy 393
ssh policy 393
SSL VPN 226
star display, Firebox System Manager 35
static NAT. See NAT, static
status passphrase
as log encryption key 16

changing 64–65
described 18, 64
setting 16
Status Report tab (Firebox System Manager) 48–49
Steel Belted RADIUS 128
strip (proxy action) 162
strong encryption. See encryption, strong
Sun RPC policy 393
Support Logs dialog box 49
support services, online 25
SYN flood attacks 137
syslog
described 394
facility 85
logging, enabling 84
policy 394
system files, location of 375

T

TACACS policy 394
TACACS+ policy 394
TCP connections 394
TCP policy 394
TCP proxy
and Gateway AntiVirus 310
and High Availability 348
and intrusion prevention 183
and Intrusion Prevention Service 314, 315, 317
configuring 183
configuring general settings for 183
described 183, 400
TCP segment adjustment, setting 77
TCP SYN checking, enabling 76
TCPmux service 142
TCP-UDP policy 395
Technical Support
assisted support 28
Firebox Installation Services 29
LiveSecurity Gold Program 29
LiveSecurity Service 28
users forum 26, 27
VPN Installation Services 29
telnet policy 395
third-party authentication server. See authentication or name of third-party server
Timbuktu policy 395
Time Exceeded setting (ICMP) 76
Time Filters dialog box 187
Time policy 395
time zone for Firebox, setting 62
timeout duration for Firebox 18
toolbar. See WatchGuard toolbar
traceroute command for source of messages 40
traceroute policy 396
traffic
viewing Firebox 35
volume indicator for 36
Traffic Monitor
blocking source/destination of message 40
copying messages in 40
issuing ping and traceroute command in 40
limiting messages 38
Traffic Monitor tab (Firebox System Manager) 38–40
training and certification 26, 29
Transmission Control Protocol (TCP) 183
triangle display, Firebox System Manager 35
trusted interface
and WINS/DNS servers 107
cabling and 66
configuring 98–100
described 10
Tunnel Properties dialog box 241
tunnel switching 231
tunnels
monitoring 6, 37
protocols for 226
See also VPN tunnels
viewing status of 36
Type of Service (TOS) bits 76

U

UDP policy 395
unhandled packets 137
unlocking e-mail attachments 312
Update Device dialog box 218, 238, 263, 266
Update Firmware wizard 260
upgrades
and High Availability 348
and LiveSecurity Service 19, 24
and Quick Setup Wlzard 14
Fireware 20
user authentication. See authentication
users
and Active Directory authentication 131
and Firebox authentication 123
and LDAP authentication 129
and RADIUS server authentication 127
and SecurID authentication 128
assigning to authentication groups 123, 126
authenticating remote 124
configuring a policy for authentication of 132–133
list of authenticated 49
online forum for 26
viewing in HostWatch 54
users forum 26
UUCP policy 396

V

virtual private networks. See VPNs
viruses
defending against. See Gateway AntiVirus
information about new 24
seeing number found 37
VPN Installation Services 29
VPN Manager Access page 257
VPN Resource dialog box 238
VPN tunnels
and gateways 243
authentication/encryption types for 239
configuring with manual security 246
creating policies for 250
creating with Add VPN Wizard 240
creating with WatchGuard System Manager 237, 240
drag-and-drop creation 240
editing 241
removing from WatchGuard System Manager 241
without drag-and-drop 240–241

VPNs
access control for 229
and Any policy 379
and IP addressing 228
and NAT 229
and strong passwords 227
and WatchGuard System Manager 233
authentication methods for 227
described 226
design considerations 230
global settings 75
graphing events regarding 41
managed. See BOVPN with WatchGuard System Manager
manually configured. See BOVPN with Manual IPSec
monitoring 220
network topology 229
scenarios 234
steps in creating 237
types of 232
using 1-to-1 NAT when networks use same IP 117

W

WAIS policy 396
WatchGuard Certified Training Partners 29
WatchGuard Firebox System
and managed clients 210
and Management Server 213
described 2
documentation for 2
file locations for 377
log files created with 95
ports for Log Server 20
WatchGuard Log Server Configuration dialog box 82
WatchGuard Management Access page 256
WatchGuard Management Server. See Management Server
WatchGuard PPTP policy icon 281
WatchGuard System Manager
and authentication via certificates 234
and IPSec tunnels 233
and VPNs 233
described 1
Device Management tab 5
Device Status tab 4
installing 9–22
location of data files for 375
monitoring tunnels in 6
package contents 9
servers 1
setting up management station 13
starting 17
user interface 4
viewing connection status in 6
WatchGuard toolbar
and Log Server 82
and Management Server 199
and WebBlocker Server 290
described 2, 4
icons on 4
WatchGuard users forum 26, 27
WCTP 29
Web Quick Setup Wizard
and secondary networks 21
described 15
troubleshooting 15
using 15
using for recovery 15
web sites
anonymizer 293, 294
filtering 3, 289
selecting categories to block 293, 294
viruses in 308
WebBlocker
adjusting cache size for 296
automatically downloading database 291
configuring 293–296
creating exceptions for 295–296
described 3, 289
downloading database 290
installing license for 289
prerequisites 290
scheduling an action for 297
scheduling hours 297
selecting policies for 292
selecting site categories to block 293, 294
setting timeout value 296
time zone for 62
WebBlocker Configuration dialog box 294
WebBlocker Server
adding additional 292
adding new 294
described 1
icon on toolbar for 4
installing 290
installing on computers with desktop firewalls 20
where to install 13
WebBlocker utility 290
well-known policies 379
WFS 377
and managed clients 210
and Management Server 213
described 2
documentation for 2
log files created with 95
ports for Log Server 20
WG-Auth policy 397
WG-Firebox-Mgmt policy 397
WG-Logging policy 397
WG-Mgmt-Server policy 397
WG-SmallOffice-Mgmt policy 398
WG-WebBlocker policy 398
WHOIS policy 398
Windows 2000
and LDAP-SSL 387
preparing for RUVPN with PPTP 286
Windows networking 392
Windows XP, preparing for RUVPN with PPTP 285
Winframe policy 396
WINS servers
addresses for 107
configuring 280
WSM. See Watchguard System Manager

X

X Font server 142
X Window System 142
X11 policy 398

Y

Yahoo Messenger policy 398